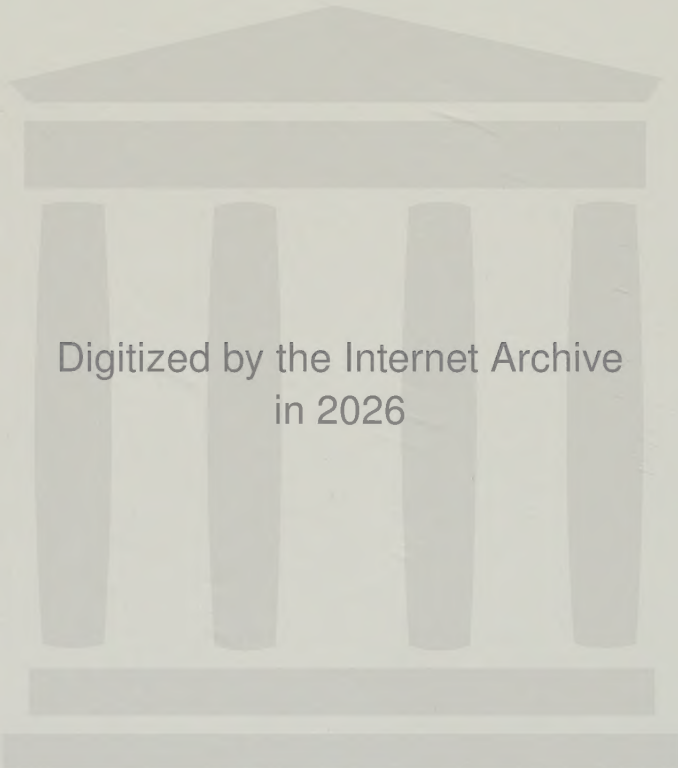


ÜBER EINKLASSIGE GESCHLECHTER
POSITIV-DEFINITER BINÄRER QUADRATISCHER FORMEN

D i s s e r t a t i o n
zur Erlangung des Grades
'D o k t o r
d e r N a t u r w i s s e n s c h a f t'
am Fachbereich Mathematik
der Johannes Gutenberg-Universität
in Mainz

Michael Kassner
geb. in Simmern

Mainz 1981



Digitized by the Internet Archive
in 2026

ÜBER EINKLASSIGE GESCHLECHTER
POSITIV-DEFINITER BINÄRER QUADRATISCHER FORMEN

D i s s e r t a t i o n
zur Erlangung des Grades
"D o k t o r
d e r N a t u r w i s s e n s c h a f t"
am Fachbereich Mathematik
der Johannes Gutenberg-Universität
in Mainz

Michael Kassner
geb. in Simmern

Mainz 1981



Dekan: Prof. Dr. H. Mülthei

Erster Berichterstatter: Prof. Dr. A. Pfister

Zweiter Berichterstatter: Prof. Dr. G. Hofmeister

Tag der mündlichen Prüfung: 23. Juni 1981

Für meinen Sohn

Sebastian

INHALT:

Einleitung

I.	Bezeichnungen und Hilfsmittel.....	1
	A. Gitter.....	1
	B. Klasse und Geschlecht.....	3
	C. Darstellungen.....	4
II.	Verallgemeinerte Transformationen, die die Klassenzahl nicht erhöhen.....	8
	A. Gitter (L, A, m, t)	8
	B. Das Geschlecht von (L, A, m, t)	13
	C. Darstellungen mit Nebenbedingungen.....	17
	D. Klassenzahlabschätzung im binären Fall.....	21
III.	Binäre quadratische Formen.....	24
	A. Die Klassengruppe.....	24
	B. Geschlechter.....	26
IV.	Einklassige binäre Geschlechter.....	31
	A. Primzahldarstellung.....	31
	B. Angenehme Gitter.....	39
	C. Kongruenzbedingungen für einklassige Geschlechter...	40
	D. Summen von drei Quadraten.....	43
V.	Reduktion auf Fundamentaldiskriminanten.....	54
VI.	Numerische Ergebnisse.....	61

Literaturverzeichnis

EINLEITUNG

Nach dem Satz von Hasse-Minkowski sind zwei rationale quadratische Formen über $\mathbb{Q}$ äquivalent, falls sie lokal, d.h. über den p -adischen Zahlen $\mathbb{Q}_p$ (p prim oder ∞) äquivalent sind. Ein Analogon für ganzzahlige Äquivalenz gibt es i.a. nicht. Somit ist das Geschlecht - die Menge der zu einer Form f lokal-ganz äquivalenten quadratischen Formen - von Interesse; $c(f)$ gibt die Anzahl der Klassen im Geschlecht von f an. Für einklassige Geschlechter ($c(f) = 1$) gilt also weiterhin ein "Lokal-Global-Prinzip".

G.L. Watson benutzte Transformationen, die die Klassenzahl c nicht erhöhen, zum leichteren Auffinden der (endlich vielen) positiv-definiten einklassigen Geschlechter mit mehr als zwei Variablen. Seine Methoden funktionieren bei binären quadratischen Formen nicht mehr. Hier beeinflusst der enge klassische Zusammenhang zu quadratischen Zahlkörpern sehr stark die Theorie (Kap. III).

Einklassige Geschlechter positiver binärer quadratischer Formen werden in dieser Arbeit auf verschiedene Weise charakterisiert. Dabei steht - im Gegensatz zur Literatur - der weitere Klassenbegriff im Vordergrund. Dies ist auch bei höherdimensionalen quadratischen Formen üblich und erweist sich in diesem Zusammenhang als geeignet. Eine dieser Beschreibungen geht auf Eulers "formulae idoneae" $f = x^2 + dy^2$, $d > 0$, zurück. Diese f haben die Eigenschaft, daß $n = x^2 + dy^2$ mit $n > 1$ und $ggT(x,y) = ggT(n,4d) = 1$ prim ist, falls im wesentlichen nur eine solche Darstellung in ganzen Zahlen x,y existiert. Eine für damalige Zeiten große Primzahl entdeckte Euler mit $18518809 = 197^2 + 1848 \cdot 100^2$. Näheres dazu findet sich bei Steinig (St). In einer Verallgemeinerung der Ergebnisse von Grube (Gr) zeigt sich, daß die einklassigen

Geschlechter genau die "formulae idoneae" $ax^2+bxy+cy^2$ sind und ax^2+bx+c - bis auf einen Teiler der Diskriminante - eine niedrige Primzahlpotenz ist, falls x klein ist (s. Satz 39 u. 42).

Desweiteren wird bewiesen, daß positive binäre Formen, die hinreichend große natürliche Zahlen über $\mathbb{Z}$ darstellen, falls lokal-ganze Darstellungen existieren, einklassiges Geschlecht haben (Satz 47).

Eine Verallgemeinerung der Ergebnisse Watsons liefert u.a. die Monotonie von Klassenzahlen der Geschlechter von Darstellungen unter bestimmten Transformationen. Damit läßt sich ein Zusammenhang zwischen Darstellungen natürlicher Zahlen durch ternäre quadratische Formen mit linear homogenen Nebenbedingungen und oberen Abschätzungen der Klassenzahl c binärer Formen herstellen. (s. Kap. II). Zusammen mit dem Wissen über einklassige Geschlechter führt dies zu einer näheren Beschreibung der endlich vielen Zahlen $n \in \mathbb{N}$, $4 \nmid n$, die zwar Summe dreier - aber nicht paarweise verschiedener positiver - Quadrate sind (s. Kap. IV). Satz 57 zeigt, daß jedes solche n - bis auf 9,18,25,27,99 - quadratfrei ist, Satz 59 gibt alle $n \leq 2,5 \cdot 10^6$ an.

Außerdem werden - bei numerischen Rechnungen praktische - Bedingungen für die Diskriminante d einer binären Form mit Klassenzahl 1 angegeben, wie z.B.

$\left(\frac{-d}{p}\right) \neq 1$, falls p eine Primzahl $\leq \sqrt[4]{d/4}$ (s. Kap. IV).

Solche Kriterien ermöglichten es, mit einem Computer alle Diskriminanten unterhalb 10^7 zu untersuchen.

Durch eine im wesentlichen bekannte Formel, die den Zusammenhang zwischen den Klassenzahlen pro Geschlecht von Formen der Diskriminanten d und f^2d , $f \in \mathbb{N}$ herstellt, wird das Problem auf Fundamentaldiskriminanten zurückgeführt.

Die Ergebnisse werden tabellarisch dargestellt (s. S. 66).

Mit Hilfe eines Satzes von Tatzawa ergibt sich die Schranke $5,2 \cdot 10^{11}$, über der höchstens noch eine Fundamentaldiskriminante $d > 0$ zu einklassigem Geschlecht liegen kann (s. Satz 66).

Wie heute üblich wird die Sprechweise der quadratischen Gitter verwendet.

I. BEZEICHNUNGEN UND HILFSMITTEL

Abkürzend für die Körper der rationalen und reellen Zahlen schreiben wir $\mathbb{Q}$ und $\mathbb{R}$, für den Ring der ganz-rationalen Zahlen $\mathbb{Z}$, für die Menge der positiven Primzahlen in $\mathbb{Z}$ $\mathbb{P}$.

Falls $p \in \mathbb{P}$, so bezeichnet $|\cdot|_p$ eine p -adische Bewertung von $\mathbb{Q}$. Der durch eine Vervollständigung von $(\mathbb{Q}, |\cdot|_p)$ entstehende Körper $(\mathbb{Q}_p, |\cdot|_p)$ enthält den lokalen Ring $\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$; sei $\mathbb{Z}_\infty := \mathbb{Q}_\infty := \mathbb{R}$.

A. Gitter

Sei R ein Integritätsbereich mit Quotientenkörper k , $\text{char } k \neq 2$, $R' \supseteq R$ ein weiterer Integritätsbereich und M ein R -Modul, so entsteht aus M durch Konstantenerweiterung ein R' -Modul $M' = R'M = R' \otimes_R M$.

M sei R -Untermodul eines n -dimensionalen k -Vektorraumes V . Falls ein freier R -Modul $F \subseteq V$ vom Rang n und ein $a \in k^\times$ existiert mit $aF \subseteq M \subseteq F$, dann heißt M Gitter auf V .

Ist speziell R ein Hauptidealring - was von nun an vorausgesetzt wird -, so folgt aus dem Elementarteilersatz (z.B. OM, 81:11, S. 214), daß das Gitter M frei vom Rang n ist.

Ein R -Gitter L heißt quadratisches Gitter, falls L in einem endlichdimensionalen quadratischen k -Raum (V, q) , $V = kL$ liegt.

Die zur quadratischen Form $q: V \rightarrow k$ gehörende symmetrische Bilinearform b sei durch

$q(x + y) = q(x) + q(y) + b(x, y)$ für alle $x, y \in V$ definiert.

Für eine R -Basis $(e_1, \dots, e_n)$ von L bezeichnet

$d(e_1, \dots, e_n) := \det(b(e_i, e_j))$ und $dL := d(e_1, \dots, e_n) \bmod R^{\times 2}$ die Diskriminante der Basis bzw. des Gitters. dL soll auch als ein Vertreter seiner Quadratklasse interpretiert werden, also $dL \in k$.

L bzw. V seien von nun an regulär, d.h. $dL \neq 0$. Weiterhin sollen ωL und ωL die von $2q(L)$ bzw. $b(L, L)$ erzeugten Ideale in R sein, nL und sL entsprechend erzeugende Elemente dieser Ideale, $Nm(L) := \frac{nL}{2}$.

L heißt modular, wenn $\frac{dL}{(sL)^n} \in R^*$, primitiv, wenn $Nm(L) \in R^*$.

Falls V regulär ist, gibt es (s. Kn, S. 2) zu jeder Basis $B = (e_1, \dots, e_n)$ von L eine duale Basis

$B^{\#} = (e_1^{\#}, \dots, e_n^{\#})$ von V mit

$$(1) \quad b(e_i, e_j^{\#}) = \delta_{ij} \quad , \quad i, j \in \{1, \dots, n\}$$

$B^{\#}$ ist eine Basis des dualen Gitters $L^{\#} = \{x \in V \mid b(x, L) \subseteq R\}$

Es ergibt sich

$$(2) \quad e_j^{\#} = \sum_{i=1}^n b(e_i^{\#}, e_j^{\#}) e_i \quad , \quad j \in \{1, \dots, n\}$$

und damit insbesondere

$$(b(e_i^{\#}, e_j^{\#}))_{ij} = (b(e_i, e_j))_{ij}^{-1} \quad , \quad dL^{\#} = dL^{-1} \quad .$$

Außerdem gilt

$$(3) \quad \frac{dL}{(sL)^{n-1}} L^{\#} \subseteq L \quad . \text{ Formel (3) folgt aus (2) und}$$

$$\frac{dL}{(sL)^{n-1}} (b(e_i^{\#}, e_j^{\#}))_{ij} = \frac{\text{adj}(b(e_i, e_j))_{ij}}{(sL)^{n-1}} \in R^{\frac{n \times n}{n-1}} .$$

B. Klasse und Geschlecht

Zwei quadratische R -Moduln (M_i, q_i) , $i=1,2$ heißen isometrisch, falls ein R -Isomorphismus $u: M_1 \rightarrow M_2$ existiert mit $q_1(x) = q_2(ux)$ für alle $x \in M_1$. Die Menge dieser Isometrien u sei $O(M_1, M_2)$, $O(M) := O(M, M)$.

Zwei Gitter $L_i \subseteq V_i = kL_i$ sind isometrisch ($L_1 \cong_{\mathbb{R}} L_2$), falls ein $u \in O(V_1, V_2)$ existiert mit $uL_1 = L_2$. Wir schreiben auch $L = \langle b(e_i, e_j) \rangle_{ij}$, wenn $(e_1, \dots, e_n)$ Basis von L ist, für $n=2$ zusätzlich $L = (q(e_1), b(e_1, e_2), q(e_2))$.

Wenn L ein Gitter auf V ist, so bezeichnet $\text{cls } L$ die Menge der Gitter auf V , die zu L isometrisch sind. $\text{cls}^+ L \subseteq \text{cls } L$ sei die Menge der Gitter $L' \subseteq V$, für die ein $u \in O^+(V) = \{v \in O(V) \mid \det v = 1\}$ mit $uL = L'$ existiert; L' heißt im engeren Sinn isometrisch zu L (in Zeichen $L' \cong_{\pm} L$).

Zwei quadratische $\mathbb{Z}$ -Gitter L und K gehören zum selben Geschlecht, wenn $L_p := \mathbb{Z}_p L \cong \mathbb{Z}_p K =: K_p$ für alle $p \in \mathbb{P} \cup \{\infty\}$; dabei sind die quadratischen Formen in natürlicher Weise von L auf L_p (bzw. K auf K_p) fortgesetzt.

Diese Definition impliziert, daß mit K auch jedes $K' \cong K$ zum Geschlecht von L gehört.

Aus dem Satz von Hasse-Minkowski (OM, 66:4, S. 189) folgt, daß zu gegebenem K im Geschlecht von $L \subseteq V$ ein $K' \cong K$ mit $K' \subseteq V$ gefunden werden kann. Bei Untersuchung bis auf Isometrie genügt es daher gen L := $\{K \subseteq \mathbb{Q}L \mid K \text{ im Geschlecht von } L\}$ zu betrachten.

Es gilt sogar:

1. LEMMA: Sei $T \subseteq \mathbb{P}$, T endlich, L ein quadratisches $\mathbb{Z}$ -Gitter, $K \in \text{gen } L$. Dann gibt es ein $K' \in \text{cls}^+ K$ mit

$$K'_p = L_p \quad \text{für alle } p \in T.$$

(Beweis: OM, 102:4, S. 299) ●

Für $K \in \text{gen } L$ gilt $dL = dK$, $\Delta L = \Delta K$ und $\mathfrak{u}L = \mathfrak{u}K$, weil dies lokal so ist.

Da zu gegebenem dL und ΔL nur endlich viele Isometrie-klassen quadratischer $\mathbb{Z}$ -Gitter existieren (Kn , VII-1-(19.3)), sind die Klassenzahlen

$$\begin{aligned} c(L) &:= \# \text{ gen } L/\cong & \text{und} \\ c^+(L) &:= \# \text{ gen } L/\cong^+ & \text{endlich.} \end{aligned}$$

C. Darstellungen

Seien L und K wieder R -Gitter. L stellt K dar ($L \rightarrow K$), wenn ein $K' \cong K$ mit $K' \leq L$ existiert. Falls $kK \leq kL$, ist dies nach dem Fortsetzungssatz von Witt (OM, 42:17, S.98) äquivalent mit der Existenz eines $L' \in \text{cls } L$ mit $K \leq L'$. Falls K' direkter Summand in L ist, so heißt die Darstellung primitiv ($L \rightarrow K$). Im Sonderfall $K = Rv$, $q(v) = n$ schreiben wir auch $L \rightarrow n$ bzw. $L \rightarrow n$.

Die Eigenschaft " $\mathbb{Z}v$ liegt primitiv in L " ist gleichbedeutend damit, daß die Entwicklungskoeffizienten von v nach einer Basis von L teilerfremd sind (vgl. vdW, S.278 ff).

2. BEISPIEL: Seien L und K $\mathbb{Z}$ -Gitter, $L \cong (1,0,11)$,
 $K \cong \langle 2 \cdot 3 \rangle$. L stellt K über $\mathbb{Q}$ und $\mathbb{Z}_p$, $p \in \mathbb{P} \cup \{\infty\}$ dar,
denn

$$3 = \left(\frac{8}{5}\right)^2 + 11 \cdot \left(\frac{1}{5}\right)^2 \quad (p \neq 5) \quad \text{und}$$

$$3 = \left(\frac{1}{2}\right)^2 + 11 \cdot \left(\frac{1}{2}\right)^2 \quad (p = 5) \quad .$$

Andererseits ist $L \not\supseteq K$ (d.h. $3 = x^2 + 11y^2$) über $\mathbb{Z}$
nicht lösbar.

Dieses Beispiel zeigt $c((1,0,11)) > 1$, denn es gilt:

3. SATZ: Seien L und K reguläre $\mathbb{Z}$ -Gitter, $L_p \supseteq K_p$ für
alle $p \in \mathbb{P} \cup \{\infty\}$.

- a) Es gibt ein $K' \cong K$, $K' \subseteq \mathbb{Q}L$ mit $L_p \supseteq K'_p$
für alle $p \in \mathbb{P} \cup \{\infty\}$.
- b) Sei $K \subseteq \mathbb{Q}L$. Dann gibt es ein $L' \in \text{gen } L$ mit
 $L' \supseteq K$. Sind alle lokalen Darstellungen primitiv,
so kann auch die Darstellung $L' \supseteq K$ primitiv
gewählt werden.

Beweis:

- a) Dies folgt aus Hasse-Minkowski (OM, 66:3, S. 189).
- b) Der erste Teil ergibt sich aus (OM, 102:5, S. 300).

Sei also $L' \supseteq K$, $L' \in \text{gen } L$, $V = \mathbb{Q}L$. Es gibt eine
endliche Menge $T \subseteq \mathbb{P}$, so daß K_p direkter Summand von
 L'_p für alle $p \in \mathbb{P} \setminus T$.

Für $p \in T$ ist nach Voraussetzung K_p direkter Summand
in $u_p L'_p$ für ein $u_p \in \mathcal{O}(V_p)$. Nun existiert nach

(OM, 81:14, S. 218) ein $\mathbb{Z}$ -Gitter L'' auf V mit

$$L''_p = \begin{cases} L' & \text{für } p \in T \\ \cup_p L'_p & \text{für } p \notin T \end{cases},$$

also ist $L'' \in \text{gen } L$.

Ein R -Gitter G ($R = \mathbb{Z}$ oder $\mathbb{Z}_p$) ist direkter Summand eines Gitters H genau dann, wenn $kG \cap H = G$ ist.

Die nichttriviale Richtung dieser Bemerkung folgt, indem man mit (OM, 81:3, S. 211) eine Basis $(e_1, \dots, e_n)$ von H wählt mit $\langle e_1, \dots, e_r \rangle_k = kG$ und $G = kG \cap H = \langle e_1, \dots, e_r \rangle_R \subset H$ folgert.

In unserem Fall ist also $\mathbb{Q}_p K_p \cap L''_p = K_p$ für alle p . Dies zeigt auch $K_p \subseteq (\mathbb{Q}K \cap L'')_p \subseteq \mathbb{Q}_p K_p \cap L''_p = K_p$, also $K_p = (\mathbb{Q}K \cap L'')_p$ für alle p und damit $K = \mathbb{Q}K \cap L''$ (OM, S. 218). Daraus ergibt sich wiederum, daß K direkter Summand in L'' ist. ●

Satz 3 zeigt insbesondere, daß quadratische $\mathbb{Z}$ -Gitter L mit einklassigem Geschlecht ($c(L) = 1$) ein "Lokal-Global-Prinzip" für (primitive) Darstellungen besitzen. Diese Eigenschaft erleichtert die Antwort auf Darstellungsfragen erheblich, da lokal genügend einfache Kriterien zur Hand sind (vgl. z.B. das Buch von OM).

Betrachten wir zum Schluß dieses Kapitels die Anzahl der einklassigen Geschlechter.

Im indefiniten Fall, falls also für den tragenden $\mathbb{Q}$ -Vektorraum V ein $0 \neq v \in \text{RV}$ mit $q(v) = 0$ existiert,

gibt es unendlich viele einklassige Geschlechter.
Dies zeigt z.B.

4. LEMMA: Sei L reguläres $\mathbb{Z}\mathbb{Z}$ -Gitter auf einem indefiniten quadratischen Raum V , $n = \dim V \geq 3$, $q(L) \leq \mathbb{Z}$,
 $p^{\frac{n(n-1)}{2}} \nmid dL$ für alle $p \in \mathbb{P}$. Dann folgt $c(L) = 1$.

Beweis: (Kn, VIII, S. 11- 14) ●

Unendlich viele Beispiele für binäre $\mathbb{Z}\mathbb{Z}$ -Gitter mit einklassigem Geschlecht liefern alle indefiniten primitiven binären L mit $dL = -5 \cdot 5^{2t}$, $t \in \mathbb{N}_0$. Zu diesen Diskriminanten gibt es nämlich jeweils nur eine Klasse, wie die (+) (S. 55) entsprechende Formel für den indefiniten Fall zeigt (s. L, Satz 209, 214).

Im Gegensatz dazu gibt es im definiten Fall, $\text{rg } L \geq 2$, nur endlich viele einklassige Geschlechter (s. Kap. VI).

II. VERALLGEMEINERTE TRANSFORMATIONEN, DIE DIE KLASSENZAHL NICHT ERHÖHEN

G.L. Watson benutzte gewisse Transformationen, die die Klassenzahl nicht erhöhen, um u.a. rang $L \leq 10$ für positiv-definite $\mathbb{Z}$ -Gitter L mit $c(L) = 1$ zu beweisen (w_1, w_2, w_3). Diese Abbildungen werden hier verallgemeinert.

A. Das Gitter (L, A, m, t)

5. DEFINITION: Sei $R = \mathbb{Z}$ oder $\mathbb{Z}_p$, $p \in \mathbb{P}$ und L ein reguläres R -Gitter auf V , A ein weiteres R -Gitter, $A \subseteq V$, $m \in R \setminus \{0\}$, $t \in \{0, 1\}$.

$$(L, A, m, t) := \{x \in L \mid b(x, A) = 0, b(x, L) \subseteq mR, 2^t q(x) \in mR\}$$

6. HILFSSATZ: (L, A, m, t) wie in Def.5 ist ein R -Gitter.

Beweis:

Mit L ist auch $L \cap U$ für jeden Unterraum $U \leq V$ ein Gitter, denn es gibt nach (OM, 81:3, S. 211) eine Basis $(e_1, \dots, e_n)$ von L , $\langle e_1, \dots, e_r \rangle_k = U$ für ein $r \leq n$.

Falls $g \in k$ ein größter gemeinsamer Teiler von 1 und NmL ,

so gilt offensichtlich $\frac{1}{g} m(L \cap (kA))^\perp \subseteq (L, A, m, t) \subseteq L \cap (kA)$

($U^\perp$ bezeichnet allgemein den Orthogonalraum von U in V).

Da $L \cap kA^\perp$ ein Gitter, folgt, daß auch der R -Modul (L, A, m, t) ein Gitter ist •

Für zwei Elemente $a, b \in K$ bezeichne (a, b) einen größten gemeinsamen Teiler bzgl. R .

7. LEMMA: Sei $s = sL$, $d = dL$, $n = nL$, $r = \text{rang } L$,
 $s, d, n \in K$, $m, m' \in R$, $t, t' \in \{0, 1\}$, $t \geq t'$.

Dann gilt:

$$1) (L, A, m, t) = (L, A, m', t), \text{ falls } \frac{m}{m'} \in R^\times.$$

$$2) (uL, uA, m, t) = u(L, A, m, t), \text{ falls } u = kL, u \in O(V);$$

$$u|_K(L, A, m, t) \in O(K(L, A, m, t)), \text{ falls } u(A) = A.$$

$$3) (L, A, 2m, 1) \subseteq (L, A, m, 0) \subseteq (L, A, m, 1) \subseteq mL^\# \cap (kA)^\perp.$$

$$4) (L, A, m, t') = ((L, A, m, t), \{0\}, m, t').$$

$$5) (L, A, m, t) = (B, \{0\}, m, t), \text{ falls } L = A \perp B \text{ und } A \text{ regulär.}$$

$$6) (L, A, m, t) = m(L^\# \cap kA^\perp), \text{ falls } 2^{1-t} \cdot \frac{d}{s^{r-1}} \mid m.$$

$$7) (L, A, m, 1) = \left(\frac{m}{m, s}\right) (L \cap kA^\perp) = \left(\frac{sm}{m, s}\right) (L^\# \cap kA^\perp), \text{ falls}$$

$$L \text{ modular (d.h. } \frac{d}{s^r} \in R^\times).$$

$$8) (L, A, m, 1) = L \cap kA^\perp, \text{ falls } m \mid s$$

$$(L, A, m, 0) = L \cap kA^\perp, \text{ falls } 2m \mid n.$$

$$9) (L, A, m, 1) = \left(\frac{m}{m, s}\right) (L \cap \mathbb{Q}A^\perp), \text{ falls } L \text{ } \mathbb{Z}\text{-Gitter}$$

$$\text{und } \left(\frac{m}{m, s}\right), \frac{d}{s^r} = 1.$$

Beweis:

1) und 2) ergeben sich aus der Definition.

Zu 3): Da $b(\frac{1}{m}(L, A, m, t), L) \subseteq R$, $\frac{1}{m}(L, A, m, t) \subseteq kA^\perp$,
folgt $\frac{1}{m}(L, A, m, t) \subseteq L^\# \cap kA^\perp$ und die letzte
Inklusion.

Zu 4): Für $x \in (L, A, m, t')$ gilt $b(x, L) \subseteq mR$, also auch
 $b(x, (L, A, m, t)) \subseteq mR$ und $2^{t'}q(x) \in mR$, d.h. $x \in$
 $((L, A, m, t), \{0\}, n, t')$.

Zu 5): Da A regulär und B direkter Summand, folgt $kA^\perp = kB$
und $L \cap kA^\perp = L \cap kB = B$. Außerdem ist
 $b(x, L) = b(x, B)$ für $x \in B$.

6): $(L, A, m, 1) = L \cap mL^\# \cap kA^\perp = mL^\# \cap kA^\perp$, da
nach (3) $\frac{d}{s^{r-1}} L^\# \subseteq L$, also auch $mL^\# \subseteq L$.
Damit ist auch $(L, A, m, 0) \subseteq mL^\# \cap kA^\perp$. Für $t = 0$,
 $x \in mL^\#$ ist $\frac{m}{2} L^\# \subseteq L$, also $q(x) = \frac{1}{2}b(x, x) =$
 $b(x, \frac{x}{2}) \in b(x, L) \subseteq mR$. Somit gilt Gleichheit.

7): Mit $\frac{d}{s^r} \in R^\times$ ergibt sich aus (3) $L^\# = \frac{1}{s}L$, also
 $(L, A, m, 1) = s \cdot L^\# \cap mL^\# \cap kA^\perp = \frac{sm}{(s, m)} L^\# \cap kA^\perp = \frac{m}{(s, m)} L \cap kA^\perp$.

Zu 8): $m \mid s$ impliziert $b(L, L) \subseteq sR \subseteq mR$.

$2m \mid n$ impliziert $m \mid s$ und $q(L) \subseteq \frac{n}{2} R \subseteq mR$.

9): Sei $p \in \mathbb{P}$. Falls $p \nmid (\frac{m}{s})$, so ist $(\frac{m}{s}) \in \mathbb{Z}_p^\times$,
also $m \nmid_{\mathbb{Z}_p} (m, s)$, $m \nmid_{\mathbb{Z}_p} s$. Nach 8), Lemma 11 (s.S.13)

und $(\triangleleft L)_p = \triangleleft L_p$ gilt für ein $g \in \mathbb{Z}$ mit $s \mid g$

$$\begin{aligned} \left(\frac{m}{m,s}\right) (L \cap QA^\perp)_p &= (L, A, g, 1)_p = (L_p, A_p, g, 1) = \\ &= L_p \cap QA_p^\perp = (L_p, A_p, m, 1). \end{aligned}$$

Falls $p \nmid \frac{d}{s}$, so ist L_p modular. Mit 7) und Lemma 11 (s.S.

ergibt sich $(L, A, m, 1)_p = \left(\frac{m}{m,s}\right) (L \cap QA^\perp)_p$ für alle $p \in \mathbb{P}$, und es folgt die Behauptung $\bullet$

Eine Möglichkeit der Berechnung von (L, A, m, t) liefert

8. LEMMA: Sei $L = A \oplus B \oplus C$, $e \in R \setminus \{0\}$ so, daß $e \cdot mL^\# \subseteq L$. Dann gilt

$$\begin{aligned} 2^{1-t} e(L, A, m, t) &\subseteq 2^{1-t} e(mL^\# \cap KA^\perp) \subseteq (L, A \oplus B, m, t) \oplus \\ &\quad (L, A \oplus C, m, t) \subseteq (L, A, m, t) \end{aligned}$$

Beweis:

Die erste Inklusion liefert Lemma 7, 3).

Zur zweiten Inklusion: Da V ein regulärer Raum ist, folgt für die tragenden Vektorräume der Gitter $KA^\perp = (k(A \oplus B))^\perp \oplus (k(A \oplus C))^\perp$, denn $KA = k(A \oplus B) \cap k(A \oplus C)$. Da bei regulären Räumen V für Unterräume U $\dim U^\perp = \dim V - \dim U$ gilt, ist die Summe aus Dimensionsgründen direkt.

Wir beweisen nun

$$(*) \quad mL^\# \cap KA^\perp = (mL^\# \cap k(A \oplus B)^\perp) \oplus (mL^\# \cap k(A \oplus C)^\perp)$$

Sei dazu $x \in mL^\# \cap KA^\perp$, $x = k_1 + k_2$, $k_1 \in k(A \oplus B)^\perp$, $k_2 \in k(A \oplus C)^\perp$.

$$\begin{aligned} b(k_1, L) &= b(k_1, A \oplus B \oplus C) = b(k_1, C) = b(k_1 + k_2, C) = \\ &= b(x, C) \subseteq b(x, L) \subseteq mR. \end{aligned}$$

Ebenso ist $b(k_2, L) \subseteq mR$ und damit $\frac{k_i}{m} \in L^*$.

Nun gilt für beliebige $X \subseteq L$

$2^{1-t} e(mL^* \cap kX^\perp) \subseteq (L, X, m, t)$, denn einmal ist

$2^{1-t} e(mL^* \cap kX^\perp) \subseteq L \cap kX^\perp$ nach Wahl von e , zum andern $b(mL^*, L) = mb(L^*, L) \subseteq mR$ und $q(2^{1-t} e(mL^*)) \subseteq b(e mL^*, L) \subseteq mR$.

Hieraus ergibt sich zusammen mit (*) die zweite Inklusion.

Die letzte Inklusion folgt aus der Tatsache, daß $(L, X, m, t) \subseteq (L, Y, m, t)$, falls $Y \subseteq X$ •

9. BEMERKUNG: Da $\frac{d}{s^{r-1}} L^* \subseteq L$, d, s, r wie in Lemma 7, erfüllt jedes $e \in R$ mit $\frac{d}{ms^{r-1}} | e$ die Voraussetzung von Lemma 8.

Um die Diskriminanten von (L, A, m, t) in den Griff zu bekommen, beweisen wir noch

10. LEMMA: Sei A direkter Summand von L . Dann ist

$$d(L^* \cap (kA)^\perp) \cdot R^{\times 2} = \frac{dA}{dL} \cdot R^{\times 2}.$$

Beweis:

Wenn $(e_1, \dots, e_r)$ Basis von A , $(e_1, \dots, e_n) = B$ Basis von L , $(e_1^*, \dots, e_n^*)$ die zugehörige duale Basis von L^* , so folgt nach Formel (1) $L^* \cap kA^\perp = Re_{r+1}^* + \dots + Re_n^*$.

Betrachte nun das Gitter $L' := A \perp (L^* \cap kA^\perp)$ mit Basis $B' = (e_1, \dots, e_r, e_{r+1}^*, \dots, e_n^*) =: (e_1', \dots, e_n')$.

$T = (t_{ij})_{ij}$ sei definiert durch $e_i' = \sum_{j=1}^n t_{ji} e_j$, $i = 1, \dots, n$.

Nach Formel (2) hat T Kästchenform

$$T = \left(\begin{array}{c|c} \begin{array}{ccc} 1 & & \\ & \circ & \\ & & \ddots \\ & & & 1 \end{array} & \begin{array}{c} * \\ \\ \\ \end{array} \\ \hline \begin{array}{c} \\ \\ 0 \end{array} & \begin{array}{c} \\ \\ M \end{array} \end{array} \right) \quad M = (b(e_i^*, e_j^*))_{r+1 \leq i, j \leq n}$$

Dies ergibt $dA \cdot d(L^* \cap KA^\perp) = dL' = dL \cdot (\det T)^2 =$
 $= dL \cdot (\det M)^2 = dL \cdot (d(L^* \cap KA^\perp))^2.$
 Falls $dA \neq 0$, ist A regulär und damit auch $(KA)^\perp$, also
 auch $d(L^* \cap KA^\perp) \neq 0$. Dann folgt die Behauptung durch Kürzen.
 Falls $dA = 0$, ist auch $d(L^* \cap KA^\perp) = 0$ ●

B. Das Geschlecht von (L, A, m, t)

Im folgenden wird das Geschlecht von (L, A, m, t) untersucht.

11. LEMMA: Seien L und A $\mathbb{Z}$ -Gitter, $m \in \mathbb{Z} \setminus \{0\}$, $p \in \mathbb{P}$.

Dann ist

$$(L, A, m, t)_p = (L_p, A_p, m, t) \quad .$$

Beweis:

Falls $(u_1, \dots, u_r)$ eine Basis von QA, $(u_1, \dots, u_n)$ Basis von $V = \mathbb{Q}L$,
 so gilt $\dim_{\mathbb{Q}_p}((QA)^\perp)_p = \dim_{\mathbb{Q}} QA^\perp = n - \text{rg}_{\mathbb{Q}}(b(u_i, u_j))_{i,j \leq r} =$
 $= n - \text{rg}_{\mathbb{Q}_p}(b(u_i, u_j))_{i,j \leq r} = \dim_{\mathbb{Q}_p}((QA)_p)^\perp$. Mit $(QA^\perp)_p \subseteq ((QA)_p)^\perp$
 ergibt sich $(QA^\perp)_p = (QA)_p^\perp$. Das $\mathbb{Z}_p$ -Gitter (L_p, A_p, m, t)
 auf diesem Raum $(QA^\perp)_p$ kommt damit bekanntlich von einem

$\mathbb{Z}$ -Gitter F auf $(\mathbb{Q}A)^\perp$, d.h. $F_p = (L_p, A_p, m, t)$
(vgl. z.B. OM, 81:14, Beweis Teil 1, S. 218).

Da nun $(L, A, m, t) \subseteq (L_p, A_p, m, t)$ folgt
 $(L, A, m, t)_p \subseteq (L_p, A_p, m, t)$.

Umgekehrt genügt es, $F \subseteq (L, A, m, t)_p$ zu zeigen:

Wenn $y \in F$ und $(e_1, \dots, e_r)$ ein Erzeugendensystem von L ,
dann gilt $\{b(y, e_i), 2^t q(y) \mid i=1, \dots, r\} \in m\mathbb{Z}_p \cap \mathbb{Q}$.

Damit gibt es ein $h \in \mathbb{Z}$, $p \nmid h$, so daß

$\{b(hy, e_i), 2^t q(hy) \mid i=1, \dots, r\} \in m\mathbb{Z}$. Außerdem ist

$y \in L_p \cap V$, d.h. $h'y \in L$ für geeignetes $h' \in \mathbb{Z}$, $p \nmid h'$.

Insgesamt gilt $hh'y \in (L, A, m, t)$, d.h. $y \in (L, A, m, t)_p$,
da auch $b(y, A) \subseteq b(y, A_p) = \{0\}$ ●

12. DEFINITION: Seien A, L_i reguläre quadratische R -Gitter und
 $u_i: A \rightarrow L_i$ Darstellungen, d.h. Isometrien von
 A in L_i , $i=1, 2$.

a) u_1 und u_2 heißen äquivalent (in Zeichen $u_1 \overset{\sim}{\sim} u_2$),
wenn ein $v \in O(L_1, L_2)$ existiert mit $u_2 = v \circ u_1$.
 $\text{cls}(u_1) := \{u: A \rightarrow L \mid \exists kL = kL_1, u \overset{\sim}{\sim} u_1\}$
 $\text{cls}^+(u_1) := \{u \in \text{cls}(u_1) \mid u \overset{\sim}{\sim} u_1, \text{ d.h. es existiert}$
 $\text{ein } v \in O^+(kL_1) \text{ mit } u = v \circ u_1\}$

b) Sei $R = \mathbb{Z}$. u_1 und u_2 gehören zum gleichen
Geschlecht, wenn $u_{1p} \cong u_{2p}$ für alle $p \in \mathbb{P} \cup \{\infty\}$.
Dabei ist $u_{ip}: A_p \rightarrow L_{ip}$ die von u_i induzierte
Darstellung, $i=1, 2$.

$\text{gen}(u_1) := \{u: A \rightarrow L \mid \mathbb{Q}L = \mathbb{Q}L_1, u_p \cong u_{1p}, \text{ für alle } p \in \mathbb{P},$
 $u(A) = u_1(A)\}$

$$c) c(u_1) = \# \text{ gen}(u_1)/\cong, \quad c^+(u_1) = \# \text{ gen}(u_1)/\overset{\sim}{\cong}.$$

13. BEMERKUNG: Aus den Sätzen von H.-Minkowski und Witt (OM, 66:4, S.189/42:17, S.98) folgt, daß zu gegebenem u_2 im Geschlecht von u_1 ein $u \in \text{gen } u_1$ mit $u \overset{\sim}{\cong} u_2$ existiert. Dies zeigt, daß bei der Untersuchung des Geschlechts bis auf Äquivalenz nur $\text{gen } u_1$ von Interesse ist.

14. SATZ: Sei $u: A \rightarrow L$ eine Darstellung von regulären $\mathbb{Z}$ -Gittern, $m \in \mathbb{Z} \setminus \{0\}$, $t \in \{0,1\}$. Dann beschreiben die Zuordnungen

$$T: \begin{cases} \text{gen}(u: A \rightarrow L)/\cong \mapsto \text{gen}(L, uA, m, t)/\cong \\ \text{cls}(u': A \rightarrow L') \mapsto \text{cls}(L', u'A, m, t) \end{cases}$$

und

$$T^+: \begin{cases} \text{gen } L / \overset{\sim}{\cong} \mapsto \text{gen}(L, 0, m, t) / \overset{\sim}{\cong} \\ \text{cls}^+ L' \mapsto \text{cls}^+(L', 0, m, t) \end{cases}$$

surjektive Abbildungen.

Beweis:

Lemma 7, 2) zeigt einmal die Wohldefiniiertheit von T und T^+ , zum andern zusammen mit Lemma 11

$$T(\text{gen } u/\cong) \subseteq \text{gen}(L, uA, m, t)/\cong, \quad T^+(\text{gen } L / \overset{\sim}{\cong}) \subseteq \text{gen}(L, 0, m, t) / \overset{\sim}{\cong}$$

Bleibt die Surjektivität von T und T^+ zu zeigen. Sei dazu $G \in \text{gen}(L, uA, m, t)$, $\mathbb{Q}G = \mathbb{Q}(L, uA, m, t)$, $G_p = v_p(L, uA, m, t)_p$

mit $v_p \in \mathcal{O}(\mathbb{Q}_p G_p)$ für alle $p \in \mathbb{P}$, $A = 0$ im zweiten Fall.

Da $\mathbb{Q}(uA)$ regulär, ist $V = \mathbb{Q}L = \mathbb{Q}uA \perp (\mathbb{Q}uA)^\perp = \mathbb{Q}uA \perp \mathbb{Q}G$.

Dann gibt es eine endliche Menge $S \subseteq \mathbb{P}$, so daß

$((L, uA, m, t) \perp uA)_p = L_p$ für $p \notin S$.

Sei $v_p^* \in O(V_p)$ definiert durch

$$v_p^*|_{Q_p G_p} = v_p, \quad v_p^*|(QuA)_p = \text{id}|(QuA)_p.$$

Dann gilt für $p \notin S$

$$v_p^* L_p = v_p(L, uA, m, t)_p \perp v_p^*(uA)_p = G_p \perp (uA)_p = (G \perp uA)_p.$$

Also gibt es (vgl. OM, 81:14, S. 218) ein Gitter L' auf V mit

$$L'_p = v_p^* L_p \quad \text{für alle } p \in \mathbb{P}.$$

Da $u_p(a) = v_p^* \circ u_p(a)$ für alle $a \in A$, folgt $(u(A))_p \subseteq L'_p$ für alle $p \in \mathbb{P}$, so daß $u(A) \subseteq L'$.

Definiert man $u': A \rightarrow L'$ durch $u'(a) = u(a)$ für alle $a \in A$, so gilt $u'_p = v_p^* \circ u_p$, also $u' \in \text{gen } u$. Lemma 7, 2)

und Lemma 11 zeigen $(L', u'A, m, t)_p = (L'_p, u'_p A_p, m, t) = (v_p^* L_p, v_p^* \circ u_p(A_p), m, t) = v_p^*(L_p, u_p(A_p), m, t) = v_p(L, uA, m, t)_p = G_p$ für alle $p \in \mathbb{P}$, so daß auch $T(\text{cls } u') = \text{cls } G$ und $T^+(\text{cls } L') = \text{cls } G$ ●

Unmittelbar folgt:

15. KOROLLAR: Unter den Voraussetzungen von Satz 14 gilt

$$c(u: A \rightarrow L) \geq c(L, uA, m, t) \quad \text{und}$$

$$c^+(L) \geq c^+(L, 0, m, t)$$

16. BEMERKUNG: Falls $A = \{0\}$, so ist $c(u: G \rightarrow L) = c(L)$, also $c(L) \geq c((L, \{0\}, m, t))$. Dies ist ein entscheidendes Ergebnis bei G.L. Watson (vgl. W2, Theorem 1).

C. Darstellungen mit Nebenbedingungen

17. SATZ: Sei L_1 ein reguläres $\mathbb{Z}$ -Gitter, $L_1, \dots, L_c \subseteq V = \mathbb{Q}L_1$

Repräsentanten für die Klassen im Geschlecht von L_1 ,
 m, t wie oben, $r, c \in \mathbb{N}$.

Für jedes L_j gebe es reguläre $\mathbb{Z}$ -Gitter $K_j^1, \dots, K_j^s$,
 $s = s(j)$ in V mit $\text{rang } K_j^i = r + 1$.

Dann gibt es ein $C = C(\text{gen } L_1, K_j^i, m, t)$, so daß gilt:

Für jede primitive Darstellung $u: A \rightarrow L_1$, $\text{rang } A = r$,
 folgt $c(L_1, uA, m, t) \leq C$, falls

u folgende Nebenbedingungen erfüllt:

Für alle $u': A \rightarrow L_j$, $u' \in \text{gen } u$ gibt es ein i mit
 $u'(A) \subseteq K_j^i$.

Beweis:

Sei o.E. L_1 ganz, d.h. $q(L_1) \subseteq \mathbb{Z}$.

Nach Satz 14 genügt es, die Klassen der $(L', u'A, m, t)$ zu
 zählen, wobei $u': A \rightarrow L'$, $u' \in \text{gen } u$.

Wenn $v: L' \rightarrow L''$ eine Isometrie, so ist $u'' = v \circ u' \in \text{cls } u'$,
 also nach Lemma 7, 2) $(L', u'A, m, t) \cong (L'', u''A, m, t)$. Deshalb
 müssen nur die $u': A \rightarrow L_j$ betrachtet werden, da die L_j
 ein Vertretersystem für ihr Geschlecht darstellen.

Sei abkürzend $g(L, K)$ die Anzahl der Klassen $(L, u'A, m, t)$
 mit $u': A \rightarrow L$, $u'(A) \subseteq K$, $u' \in \text{gen } u$.

Falls $v \in O(L)$, so muß $g(L, vK)$ nicht berücksichtigt werden,
 wenn $g(L, K)$ bereits gezählt wurde, denn jedes u' mit
 $u'(A) \subseteq vK$ liegt in der Klasse von $v^{-1} \circ u'$,
 $v^{-1} \circ u'(A) \subseteq K$, so daß auch $\text{cls}(L, u'A, m, t)$ schon auftrat.
 Dies ergibt

$$(4) \quad c(L_1, uA, m, t) \leq \sum_{j, L_j \rightarrow A} \sum_{K_j^i \bmod O(L_j)} g(L_j, K_j^i).$$

Obere Abschätzung für $g(L_j, K_j^i)$:

Sei $L := L_j$, $K := K_j^i \cap L_j$. Wenn man K vergrößert, gibt
 es höchstens mehr Möglichkeiten für u' , so daß nun K als

direkter Summand in L vorausgesetzt wird.

Da $u: A \rightarrow L_1$ eine primitive Darstellung und $u': A \rightarrow L \in \text{gen } u$, ist auch u' eine primitive Darstellung (vgl. Satz 3, Bemerkung im Beweis).

Wir betrachten das Gitter

$$(5) \quad G(u') := (L, (u'A) \oplus B', m, t) \oplus (L, (u'A) \oplus C, m, t),$$

wobei B' und C Gitter mit $(u'A) \oplus B' = K$, $K \oplus C = L$ sind (vgl. Lemma 8). $G(u')$ weicht eventuell etwas von $(L, u'A, m, t)$ ab.

Im folgenden werden die Klassen der $G(u')$ gezählt.

Dazu bestimmen wir zunächst die Anzahl der Geschlechter:

Sei $u_0: A \rightarrow L$, $u_0 \in \text{gen } u$ fest. Für jedes $u': A \rightarrow L$, $u' \in \text{gen } u$ gibt es $v_p' \in O(L_p)$, so daß $u_{0p} = v_p' \circ u'_p$ für alle $p \in \mathbb{P}$. Dies ergibt

$$v_p'(mL^{\#} \cap (Qu'A)^{\perp})_p = mv_p'L_p^{\#} \cap Qu_0A_p^{\perp} = (mL^{\#} \cap (Qu_0A)^{\perp})_p.$$

Aus Lemma 8 und geeigneter Wahl von e (vgl. Bemerkung 9) folgt

$$2^{1-te}(mL^{\#} \cap Qu'A^{\perp}) \subseteq G(u') \subseteq mL^{\#} \cap Qu'A_p^{\perp}, \text{ also auch}$$

$$2^{1-te}(mL^{\#} \cap Qu_0A^{\perp})_p \subseteq v_p'G(u')_p \subseteq (mL^{\#} \cap Qu_0A^{\perp})_p.$$

Da die äußeren Gitter für fast alle p übereinstimmen, gibt es ein Zwischengitter G mit $G_p = v_p'G(u')_p$ für alle $p \in \mathbb{P}$ (vgl. DM, 81:14, S. 218). Wenn $a = a(2^{1-te})$ die Anzahl der Zwischengitter angibt, gibt es also höchstens a Geschlechter von $G(u')$, $u': A \rightarrow L$.

Für jedes dieser Geschlechter, bestimmt durch $G(\bar{u})$, $\bar{u}: A \rightarrow L$, $\bar{u} \in \text{gen } u$ sind nun noch die Klassen der $G(u')$ zu zählen, für die für alle $p \in \mathbb{P}$ $v_p' \in O(L_p)$ existieren mit $v_p' \circ u'_p = \bar{u}_p$ und $v_p'G(u')_p = G(\bar{u})_p$.

Da $\text{rang } A + 1 = \text{rang } K$, $\text{rang } G(u') = \text{rang } (L, K, m, t) + 1$,
 hat $G(u')$ die Gestalt $G(u') = (L, K, m, t) \oplus \mathbb{Z}w_u$, $w_u \in G(u')$.
 Dabei ist $\pm w_u$ modulo (L, K, m, t) eindeutig bestimmt.
 Ändert man also w_u ab,

$$w := \pm w_u + \sum x_i g_i, \quad (g_1, \dots, g_l) \text{ Basis von } (L, K, m, t),$$

$x_i \in \mathbb{Z}$, so ist

$$b(w, g_i) = \pm b(w_u, g_i) + \sum x_j b(g_j, g_i), \quad i=1, \dots, l.$$

Wählt man nun für die Matrix $B = (b(g_i, g_j))_{i,j}^1$ ein

Vertretersystem $Y_1, \dots, Y_s \in \mathbb{Z}^1$ der Restklassen mod B

($A \equiv C \pmod{B} \Leftrightarrow A - C = Bx$, $x \in \mathbb{Z}^1$), das zusätzlich
 $Y_i \not\equiv \pm Y_j \pmod{B}$ für $i \neq j$ erfüllt, so zeigt die Überlegung,
 daß zu jedem $G(u')$ ein w_u existiert mit $(w_u, g_j)_{j=1, \dots, l} = Y_i$,
 $i \in \{1, \dots, s\}$. Dabei ist i durch $G(u')$ bestimmt.

Für festes Y_i ist nun $q(w_u)$ allein durch $d(G(\bar{u}))$
 festgelegt, denn es gilt

$$(6) \quad d(G(u')) = 2q(w_u) \det B - Y_i^t (\text{adj } B) Y_i \quad \text{und}$$

$$dG(u') = dG(\bar{u}), \quad \text{da } G(u') \in \text{gen } G(\bar{u}).$$

Es gibt also höchstens soviele Klassen $G(u')$ wie
 Restklassen $Y \pmod{B}$. Diese Anzahl der Restklassen
 $Y \pmod{B}$ läßt sich z.B. durch $N = (\det B)^1 = d(L, K, m, t)^1$
 abschätzen, da $Y_1 \equiv Y_2 \pmod{B}$ aus $Y_1 \equiv Y_2 \pmod{(\det B)E_1}$
 folgt.

Insgesamt gibt es höchstens $a \cdot N$ Klassen von $G(u')$,
 $u' \in \text{gen } u$.

Zum Schluß wird die Anzahl der Klassen $(L', u'A, m, t)$
 gezählt. Dabei sei die Klasse von $G(u')$ fest, d.h. es
 existiert ein festes Gitter G und $s_u \in O(G(u'), G)$.
 Lemma 8 sagt

$$2^{1-t} eG(u') \subseteq 2^{1-t} e(L, u'A, m, t) \subseteq G(u'), \quad \text{also}$$

$$2^{1-t} e_G \subseteq 2^{1-t} e_{s_u}(L, u^*A, m, t) \subseteq G.$$

Von solchen Zwischengittern gibt es höchstens a , so daß hier höchstens a Klassen gezählt werden können.

Damit kann $g(L, K) \leq a \cdot a \cdot N$ abgeschätzt werden, wobei a und N unabhängig von A sind. Formel (4) liefert die Behauptung ●

18. SATZ: Sei L_1 ein positiv-definites $\mathbb{Z}$ -Gitter mit den Voraussetzungen von Satz 17, $n-r \geq 2$. Dann gibt es eine Konstante $D = D(\text{gen } L_1, K_j^i, m, t)$, so daß für jede primitive Darstellung $u: A \rightarrow L_1$ mit den Nebenbedingungen aus Satz 17

$$|dA| \leq D \quad \text{folgt.}$$

Beweis:

Falls $uA \subseteq K \subseteq L_1$, so ist $(L_1, K, m, t) \subseteq (L_1, uA, m, t)$; damit $Nm(L_1, uA, m, t) \mid Nm(L_1, K, m, t)$. Da für jedes u $u(A) \subseteq K_j^i$, für gewisse i, j (vgl. Satz 17), ist also $N = |Nm(L_1, uA, m, t)| \leq M$ beschränkt.

Für $\mathbb{Z}$ -Gitter G sei $\text{prim}(G, q) := (G, \frac{1}{NmG} q)$.

Nach Lemma 8 und Lemma 10 folgt

$$m^{2(n-r)} \frac{dA}{dL_1} = d(mL_1^* \cap QuA^\perp) \mid d(L_1, uA, m, t).$$

Insgesamt berechnet sich

$$d(\text{prim}(L_1, uA, m, t)) = \frac{1}{N^{n-r}} d(L_1, uA, m, t) \geq \frac{m^{2(n-r)}}{M^{n-r}} \cdot \frac{dA}{dL_1}.$$

Kapitel V zeigt, daß für positiv-definite $\mathbb{Z}$ -Gitter G , $NmG = 1$, $\text{rang } G \geq 2$ $c(G)$ wächst, wenn $d(G)$ wächst. Satz 17 liefert damit eine Schranke für $d(\text{prim}(L_1, uA, m, t))$, also auch für dA ●

19. KOROLLAR: Sei $q(x_1, x_2, x_3)$ eine positiv-definite ternäre quadratische Form mit einklassigem Geschlecht, d.h. $c(\mathbb{Z}^3, q) = 1$.

Zu gegebenen Ungleichungen

$$(+)\quad \sum_{i=1}^s a_{ij}x_i \neq 0 \quad , \quad a_{ij} \in \mathbb{Z}, \text{ nicht alle Null,} \\ j=1, \dots, s$$

hat jedes $a \in \mathbb{N}$ eine Darstellung durch f , die (+) erfüllt, falls überhaupt eine primitive Darstellung existiert und a hinreichend groß ist.

Beweis:

Sei $a \in \mathbb{N}$ so, daß jede primitive Darstellung $v = (x_1, x_2, x_3) \in L = (\mathbb{Z}^3, q)$, $q(v) = a$ die Gleichungen $\sum a_{ij}x_i = 0$ erfüllt.

Die Lösungsmengen dieser s Gleichungen definieren Gitter $K_1^1, \dots, K_1^s$ vom Rang 2 in $\mathbb{Q}L$. Da $c(L) = 1$, sind die Voraussetzungen von Satz 17 für diese Darstellung erfüllt. Satz 18 liefert $2a = d \langle 2a \rangle \leq D$. Also gibt es nur endlich viele solcher a ●

D. Klassenzahlabschätzung im binären Fall

20. DEFINITION: Sei $0 \neq d \in \mathbb{Z}$.

- a) d heißt eine binäre Diskriminante, falls $-d$ kein Quadrat und ein reguläres binäres $\mathbb{Z}$ -Gitter L existiert mit $dL = d$ und $NmL = 1$.
- b) Eine Diskriminante d heißt Fundamentaldiskriminante (Kurz: FD), falls $\frac{d}{g^2}$, $g \in \mathbb{N}$ nur für $g = 1$ Diskriminante ist.

21. HILFSSATZ:

- a) $0 \neq d \in \mathbb{Z}$ ist eine Diskriminante genau dann, wenn $-d$ kein Quadrat und $d \equiv 0$ oder $-1 \pmod{4}$.
- b) Eine Diskriminante d ist genau dann eine FD, wenn $d \not\equiv 0, -4 \pmod{16}$ und $p^2 \nmid d$ für alle $2 \neq p \in \mathbb{P}$.
- c) Für jede Diskriminante d gibt es genau eine FD $\Delta(d)$ mit $d = \Delta(d)f^2$, $f \in \mathbb{N}$.

Beweis:

- a) Für $L \cong (a, b, c)$, $a, b, c \in \mathbb{Z}$, $\text{ggT}(a, b, c) = 1$ ist $dL = 4ac - b^2$.
- b) und c) sind klar ●

22. SATZ: Seien d, d' Diskriminanten, L ein binäres reguläres $\mathbb{Z}$ -Gitter mit $NmL = 1$, $dL = d' = f^2 d'$, $f \in \mathbb{N}$.
 Dann gibt es ein primitives $\mathbb{Z}$ -Gitter L_0 , $L_0 \geq L$ mit
 $dL_0 = d'$ und $c(L) \geq c(L_0)$ und $c^+(L) \geq c^+(L_0)$.
 Falls L ambig, d.h. falls ein $s \in O(L)$, $\det s = -1$ existiert, so ist auch L_0 ambig.

Beweis:

Sei $L \cong (a_0, b_0, c_0)$ mit $a_0, b_0, c_0 \in \mathbb{Z}$, $\text{ggT}(a_0, b_0, c_0) = 1$ und $p \in \mathbb{P}$ mit $p \mid d$.
 Betrachtet man den $\mathbb{Z}/p\mathbb{Z}$ -Raum $\bar{L} = L/pL$, so ist dieser nicht regulär und hat nach (Kn, 1.16, 2.16) die Form $\bar{L} = E_1 \perp F$, $q(F) = 0$, $\dim E_1 = \dim F = 1$. Dies zeigt die Existenz von $a, b, c \in \mathbb{Z}$ mit $L \cong (a, pb, pc)$, $p \nmid a$.

Es gelte nun weiter $p^2 \mid dL = 4pac - p^2b^2$, $p \nmid f$.

Dann folgt $p \mid c$: $p = 2 \nmid c$ ergäbe $(2^3 \parallel dL \text{ oder}$

$\frac{dL}{4} \equiv 1 \pmod{4}$) ; somit wäre d' keine Diskriminante.

Mit $p \mid c$ ist $c = pc'$, $c' \in \mathbb{Z}$, $L \cong (a, pb, p^2c')$.

Damit ergibt sich direkt:

$$L_1 := (L, \{0\}, p, 0) = (p^2a, p^2b, p^2c'),$$

$$L_2 := (L_1, \frac{1}{p^2}q) = (a, b, c'),$$

$$\text{ggT}(a, b, c') = 1, \quad dL_2 = \frac{dL}{p^2}$$

und $L_2 \hookrightarrow L$.

Korollar 15 liefert $c(L_2) \leq c(L)$ und $c^+(L_2) \leq c^+(L)$.

Falls L ambig, dann folgt nach Lemma 7, 2), daß L_1

und L_2 ambig sind.

Ist $|dL_2| > |d'|$, so wird mit L_2 analog verfahren.

Nach endlich vielen Schritten ist das gesuchte L_0

gefunden ●

23. BEMERKUNG: Satz 22 ist der Spezialfall eines

Ergebnisses von Watson (s. W1, Theorem 4, S. 580).

III. BINÄRE QUADRATISCHE FORMEN

A. Die Klassengruppe

Es gibt einen klassischen Zusammenhang zwischen der Theorie binärer quadratischer Formen und der Theorie quadratischer Zahlkörper, welcher hier kurz dargestellt werden soll (vgl. auch entspr. Abschnitt bei J).

Sei im folgenden $d \in \mathbb{Z}$, $-d$ kein Quadrat und $V_0 := \mathbb{Q}(\sqrt{-d})$ mit Norm N , $N(x) = x\bar{x}$, $x \in V_0$, $\bar{x}$ das Konjugierte von x .

(V_0, N) ist ein quadratischer $\mathbb{Q}$ -Raum mit zugehöriger Bilinearform $b(x, y) = \text{Sp}(x\bar{y})$, wobei Sp die Spur.

24. DEFINITION:

- a) Zwei quadratische $\mathbb{Q}$ -Räume (oder auch $\mathbb{Z}$ -Gitter) (V_i, q_i) , $i=1,2$ heißen ähnlich, wenn ein $a \in \mathbb{Q}$, $a > 0$ existiert mit $(V_1, q_1) \cong (V_2, aq_2)$.
- b) Zwei Gitter L und K auf V_1 heißen ähnlich im engeren Sinn, falls die Isometrie $(L, q_1) \cong (K, aq_1)$ positive Determinante besitzt.

25. BEMERKUNG: Jeder binäre reguläre $\mathbb{Q}$ -Raum V mit binärer Diskriminante d , V positiv-definit, falls V definit, ist ähnlich zu V_0 . Jedes Gitter L auf V ist ähnlich zu einem Gitter auf V_0 . Sei $V = \mathbb{Q}L$ nun immer positiv, falls V definit.

26. LEMMA: Zwei binäre Gitter L und K auf V_0 sind genau dann ähnlich im engeren Sinn, wenn ein $\alpha \in V_0$, $N(\alpha) > 0$ existiert mit $L = \alpha \cdot K$.

Beweis:

Seien L und K im engeren Sinn ähnlich, $u \in GL(V_0)$ mit $u(L) = K$, $N(ux) = aN(x)$ für alle $x \in L$, $0 < a \in \mathbb{Q}$, $\det u > 0$.

Dann ist $\beta^{-1}u \in O^+(V_0)$ für ein $0 \neq x_0 \in L$, $\beta := \frac{ux_0}{x_c}$;

also wie man leicht zeigt $\beta^{-1}u = \varepsilon \cdot$, wobei $\varepsilon \cdot$ die Multiplikation mit $\varepsilon \in V_0$, $N(\varepsilon) = 1$ bedeutet.

Dies ergibt $\alpha L = K$, $\alpha := \beta \cdot \varepsilon$, $N(\alpha) > 0$.

Die umgekehrte Beweisrichtung ist klar •

Wir wollen unter $D(L)$ und $N(L)$ die (algebraische) Diskriminante bzw. Norm des Gitters $L \subseteq V_0$ verstehen (s. BS, S. 110 oben bzw. S. 142 Def.).

27. LEMMA: Sei $L \subseteq V_0$, $\alpha_L := \{ \alpha \in V_0 \mid \alpha L \subseteq L \}$

der Multiplikatorring von L , $\text{prim } L := (L, \frac{1}{|Nm(L)|} \cdot N)$.

Dann gilt:

- a) $|Nm(L)| = N(L)$
- b) $d(L) = -D(L)$
- c) $d(\text{prim } L) = d(\alpha_L)$

Beweis:

- a) Sei o.E. $L = \mathbb{Z} \oplus \mathbb{Z}\gamma$, $\gamma \in V_0$. Dann folgt mit (BS, § 7.4, Lemma 1, S. 153) $\alpha_L = \mathbb{Z} \oplus \mathbb{Z}a\gamma$, wobei $0 < a \in \mathbb{Q}$ der Hauptnenner von $N(\gamma)$ und $\text{Sp}(\gamma)$. Es ergibt sich

$$N(L) = \frac{1}{a} = \text{ggT}(N(1), \text{Sp}(1 \cdot \overline{\gamma}), N(\gamma)) = |NmL|.$$

- b) Ergibt sich aus der Definition von d und D .

$$c) d(\text{prim } L) = \frac{1}{(NmL)^2} dL = - \frac{1}{N(L)^2} D(L) = -D(\alpha_L) = d(\alpha_L) \bullet$$

28. SATZ: Sei $d \in \mathbb{Z}$ eine binäre Diskriminante, $\mathcal{O}$ ein Multiplikatorenring in V_0 mit $d(\mathcal{O}) = d$, H die Gruppe der engeren Ähnlichkeitsklassen von Gittern $L \subseteq V_0$, $\mathcal{O}_L = \mathcal{O}$ (s. BS, S. 155, 156 und Lemma 26), $K^+(d)$ die Menge der engeren Isometrieklassen primitiver binärer $\mathbb{Z}$ -Gitter (positiv-definit, falls definit) mit Diskriminante d .

Dann induziert die Zuordnung $L \mapsto \text{prim } L$ eine Bijektion $H \leftrightarrow K^+(d)$.

Beweis:

Wohldefiniertheit und Injektivität der Abbildung $H \rightarrow K^+(d)$ folgen aus Lemma 26 und Lemma 27.

Falls L_0 ein binäres primitives $\mathbb{Z}$ -Gitter, $d(L_0) = d$ so gibt es ein $L \subseteq V_0$, L ähnlich zu L_0 . Dies impliziert $d(\mathcal{O}_L) = d(\text{prim } L) = d(L_0)$ und damit $\mathcal{O}_L = \mathcal{O}$, da ein Multiplikatorenring allein durch seine Diskriminante bestimmt ist (s. BS, § 7.1, S. 148, 149). Somit folgt die Surjektivität. ●

29. BEMERKUNG: Die Bijektion $H \leftrightarrow K^+(d)$ macht $K^+(d)$ zu einer endlichen abelschen Gruppe. Die Elemente von $K^+(d)$ sollen im folgenden auch mit cls^+L , L binär und primitiv, bezeichnet werden.

B. Geschlechter

30. LEMMA: Seien L, K primitive binäre $\mathbb{Z}$ -Gitter auf V , $L \ni a \in \mathbb{Z} \setminus \{0\}$, $dL = f^2 \Delta$, $f \in \mathbb{N}$, Δ FD, $\text{ggT}(a, f) = 1$. Dann ist $K \in \text{gen } L$ genau dann, wenn

$$dL = dK, \quad K \ni w^2 a \quad \text{für ein } w \in \mathbb{Z} \text{ mit } \text{ggT}(w, f) = 1.$$

Beweis:

Sei $K \in \text{gen } L$, o.E. $L_p = K_p$ für alle $p \nmid f$ (Lemma 1).

Dann gibt es $h_p \in \mathbb{Z}$ mit $h_p L \subseteq K$, $p \nmid h_p$ für $p \nmid f$.

Mit $w := \prod_{p \nmid f} h_p$ folgt $wL \subseteq K$, $(w, f) = 1$ und $K \supseteq w^2 a$.

Zur Umkehrung:

Falls $p \nmid f$, so sind L_p und K_p maximal und damit $L_p \cong K_p$ (OM, 91:2, S. 240).

Falls $p \mid f$, so $p \nmid a$, $p \nmid aw^2$ und $p \mid dL = dK$.

Für $p \neq 2$ folgt direkt $sL_p = sK_p = s(\langle 2a \rangle_p)$. Aber auch

$p = 2 \mid f$, $2 \mid dL$ ergibt $sL_2 = sK_2 = 2$. Somit ist nach (OM, 82:15a, S. 233) $\langle 2a \rangle_p$ orthogonaler Summand von L_p und K_p und aus Diskriminantengründen $L_p \cong K_p$ •

31. LEMMA: Seien L, K, L_i, K_i , $i=1,2$ primitive binäre

$\mathbb{Z}$ -Gitter zur Diskriminante d , $a_1, a_2 \in \mathbb{Z} \setminus \{0\}$,

$\text{cls}^+ L = \text{cls}^+ L_1 \cdot \text{cls}^+ L_2$, $\text{cls}^+ K = \text{cls}^+ K_1 \cdot \text{cls}^+ K_2 \in K^+(d)$.

a) Falls $L_i \supseteq a_i$, $i=1,2$ so folgt $L \supseteq a_1 \cdot a_2$.

b) Falls $L_i \in \text{gen } K_i$, $i=1,2$ so folgt $L \in \text{gen } K$.

Beweis:

a) Seien G_1, G_2 Gitter auf V_0 , o.E. $\text{prim } G_i = L_i$, $i=1,2$.

Dann kann auch o.E. $L = \text{prim}(G_1 \cdot G_2)$ gewählt werden.

$L_i \supseteq a_i$ bedeutet nun: Es gibt $\alpha_i \in G_i$,

$N(\alpha_i) = N(G_i) a_i$, $i=1,2$. Dies zeigt $N(\alpha_1 \cdot \alpha_2) = N(G_1 G_2) \cdot a_1 a_2$, also $L \supseteq a_1 a_2$.

b) Wähle a_1, a_2 so, daß $\text{ggT}(a_i, d) = 1$, $L_i \supseteq a_i$

(s. z.B. J, Th. 67, S. 164), w_i entsprechend Lemma 30

mit $K_i \supseteq w_i^2 a_i$, $i=1,2$.

Dann folgt nach a) $L \ni a_1 \cdot a_2$, $K \ni (w_1 w_2)^2 a_1 a_2$
und mit Lemma 30 die Behauptung ●

32. FOLGERUNG:

- a) Sei $\mathcal{O} \subseteq V_0$ der Multiplikatorenring zur Diskriminante d , $G_0 = \{ \text{cls}^+ L \in K^+(d) \mid L \in \text{gen } \mathcal{O} \}$ das sogenannte Hauptgeschlecht.
Dann ist G_0 eine Untergruppe von $K^+(d)$ und jedes Geschlecht zur Diskriminante d findet sich als Nebenklasse von G_0 wieder.
- b) Insbesondere enthält jedes Geschlecht $\text{gen } L$ primitiver binärer Gitter mit Diskriminante d gleich viele engere Klassen $c^+(d) = c^+(L \cdot)$.
- c) Falls d, d' binäre Diskriminanten, $d = f^2 d'$, $f \in \mathbb{N}$ so gilt $c^+(d) \geq c^+(d')$.

Beweis:

- a) Die Abgeschlossenheit von G_0 folgt mit Lemma 31 b) und $\mathcal{O} \cdot \mathcal{O} = \mathcal{O}$. Da $\text{cls}^+(\text{prim } L)^{-1} = \text{cls}^+(\text{prim } \bar{L})$, für $L \in V_0$ und $L \cong \bar{L}$ vermöge der Isometrie $-$, $NL = N\bar{L}$, ist G_0 auch bzgl. der Inversenbildung abgeschlossen.
Analog ergibt sich die zweite Behauptung von a).
- b) Die Behauptung folgt direkt aus a).
- c) Dies ergibt sich nun mit Satz 22 ●

33. LEMMA:

- a) $G_0 = \{ x^2 \mid x \in K^+(d) \}$
- b) $A := \{ \text{cls}^+ L \in K^+(d) \mid L \text{ ambig} \} = \{ x \in K^+(d) \mid x^2 = 1 \}$

c) $K^+(d)/_A \cong G_0$

d) Mit $a = \# A$, $g = \text{Anzahl der Geschlechter in } K^+(d)$,
 $h^+ = \# K^+(d)$, $c^+ = \# G_0$ gilt:

$$h^+ = c^+ \cdot g, \quad a = g, \quad c^+ = [K^+(d):A]$$

Beweis:

a) Dies ist der "Satz über die Duplikation" von Gauss.

$\{x^2 \mid x \in K^+(d)\} \subseteq G_0$ folgt direkt aus Lemma 31 a) und Lemma 30.

Sei nun $L \in \text{gen } \mathcal{O}$, $d \mathcal{O} = d$, $\mathcal{O}$ der Multiplikatorenring. Da $L \subseteq V_0$, gibt es eine endliche Menge $S \subseteq \mathbb{P}$ mit $L_p = \mathcal{O}_p$, falls $p \notin S$. Für $p \in S$ existieren $u_p \in \mathcal{O}^+(V_{0p})$ mit $L_p = u_p \mathcal{O}_p$. Diese u_p können durch ein $u \in \mathcal{O}^+(V_0)$ so gut approximiert werden, daß $L_p = (u \mathcal{O})_p$ für $p \in S$ (s. OM, 101:7, S. 290). Da $u = \varepsilon$, $\varepsilon \in V_0$, $N(\varepsilon) = 1$, gibt es nach "Hilbert 90" ein $\gamma \in V_0$ mit $\varepsilon = \gamma \cdot \bar{\gamma}^{-1}$. Sei das Gitter L' definiert durch

$$(L')_p = \begin{cases} \mathcal{O}_p & \text{falls } p \notin S \\ \gamma \mathcal{O}_p & \text{falls } p \in S \end{cases}.$$

Da offenbar $(L'^2)_p = ((N L')L)_p$ für alle $p \in \mathbb{P}$, folgt $L'^2 = (N L')L$, also $\mathcal{O}_{L'} = \mathcal{O}$ und $(\text{prim } L')^2 \cong L$.

b) Sei $x = \text{cls}^+(\text{prim } L) \in K^+(d)$, $L \subseteq V_0$.

$x = x^{-1}$ bedeutet, daß L im engeren Sinn ähnlich ist zu $\bar{L}$. Dies ist gleichwertig zu der Existenz eines $u \in \mathcal{O}(\text{prim } L)$, det $u = -1$, wie man leicht einsieht.

c) und d) sind klar ●

34. LEMMA: Sei L binäres primitives $\mathbb{Z}$ -Gitter.

- a) L ist genau dann ambig, wenn es eine $\mathbb{Z}$ -Basis (v_1, v_2) von L gibt mit

$$\begin{aligned} q(v_1) &= a & b(v_1, v_2) &= at \\ q(v_2) &= c & a, c &\in \mathbb{Z}, t \in \{0, 1\} \end{aligned} ,$$

d.h. $L \cong (a, at, c)$.

Falls $2^3 \parallel dL$, ist $t = 0$.

- b) Falls L ambig, so gibt es ein $a \mid dL$ mit $L \ni a$.
 c) Falls dL eine FD, so folgt aus $L \ni a$ für $a \mid dL$, daß L ambig.

Beweis:

- a) Die nichttriviale Richtung zeigt (J, Th. 52, S. 147).

Im Falle $2^3 \parallel dL$, $t = 1$ folgt $2^3 \parallel dL = 4ac - a^2$,

also $2 \mid a$, $8 \mid a^2$, $4 \mid a$, also $16 \mid dL$; dies ist ein Widerspruch.

- b) Dies folgt aus a).

- c) Falls $L = (a, b, c)$, $a \mid 4ac - b^2 = dL$, so folgt leicht $a \mid b$, falls dL eine FD. Da durch Basiswechsel $b \bmod 2a$ verändert werden kann, ist $b = at$ wie in a) möglich. ●

IV. EINKLASSIGE BINÄRE GESCHLECHTER

35. HILFSSATZ: Sei L reguläres primitives binäres $\mathbb{Z}$ -Gitter, $d = dL$ eine Diskriminante.

Dann sind folgende Aussagen äquivalent:

a) $c(L) = 1$

b) $c^+(L) = 1$, falls L ambig; $c^+(L) = 2$, falls L nicht ambig.

c) $K^+(d) = A \cup (\text{cls}^+L) \cdot A$

d) Falls $\text{cls}^+L = g_1 \cdot g_2$, $g_1, g_2 \in K^+(d)$, so ist $g_1 \in A$ oder $g_2 \in A$.

Beweis:

a) $\Leftrightarrow$ b): Falls L ambig, so ist $\text{cls}^+L = \text{cls } L$ und damit $c^+(L) = 1 \Leftrightarrow c(L) = 1$.

Falls L nicht ambig, so ist $\text{cls}^+(uL) \subseteq \text{gen } L$ für eine Spiegelung $u \in O(\mathbb{Q}L)$, $\det u = -1$, also $\text{cls}^+(L) \neq \text{cls}^+(uL)$. Somit ist offensichtlich $c^+(L) = 2 \Leftrightarrow c(L) = 1$.

b) $\Leftrightarrow$ c): Falls L ambig, so $(\text{cls}^+L) \cdot A = A$, sonst $(\text{cls}^+L) \cdot A \neq A$. Mit $c^+(L) = [K^+(d):A]$ nach Lemma 33 folgt die Behauptung.

c) $\Leftrightarrow$ d): Dies folgt elementar ●

A. Primzahldarstellung

36. HILFSSATZ: Sei $0 \neq m \in \mathbb{Z}$ und seien $L_1, \dots, L_r$ die Vertreter der (weiteren) Klassen primitiver (positiver, falls definiter) binärer $\mathbb{Z}$ -Gitter zur Diskriminante $dL_1 = d = f^2 \cdot \Delta(d)$, $f \in \mathbb{N}$,

$ggT(m, f) = 1$ für die $L_i \geq m$ gilt. Sei $\emptyset \neq B$,
 $B := \{(O(L_i) \cdot v, i) \mid q(v) = m, \mathbb{Z}v \text{ direkter Summand in } L_i, \\ i \in \{1, \dots, r\}\}$ die Menge der verschiedenen Bahnen primitiver
 Darstellungen von m , $\mu(m) := \#\{p \in \mathbb{P} \mid p \mid m, p \nmid d\}$.
 Dann ist

$$\# B = \begin{cases} 2^{\mu-1} & \text{falls } \mu > 0 \\ 1 & \text{falls } \mu = 0 \end{cases}$$

Beweis:

Sei $(O(L_i) \cdot v, i) \in B$ gegeben, o.E. $m > 0$
 (sonst betrachte $-q$). Ergänze v zu einer Basis (v, w)
 von L_i so, daß $0 \leq u \leq m$, $u = b(v, w)$; reduziere dazu
 $b(v, w)$ modulo $2m$ und ersetze w eventuell dann durch $-w$.

$$L_i \cong (m, u, c), \text{ wobei } c = \frac{d+u^2}{4m}.$$

Wie man leicht zeigt, liefert

$$\begin{cases} B \rightarrow M := \{u \in \mathbb{Z} \mid 0 \leq u \leq m, \text{ es gibt } c \in \mathbb{Z}, d = 4mc - u^2, \\ ggT(u, m, c) = 1\} \\ (O(L_i)v, i) \mapsto u \end{cases}$$

eine wohldefinierte bijektive Abbildung.

Da $M \neq \emptyset$, ist $d = 4mc - u^2$ lösbar. Da $\Delta(d)$ eine FD,
 $ggT(m, f) = 1$, gilt für $p \in \mathbb{P}$

$$p \mid ggT(d, m) \Rightarrow p^2 \nmid m, \quad p \nmid c.$$

Damit hat jede Lösung u von $-u^2 \equiv d \pmod{4m}$ mit
 $c = \frac{d+u^2}{4m}$ die Eigenschaft $ggT(m, u, c) = 1$.

Elementar läßt sich nun $\# B$ als Anzahl der u mit
 $0 \leq u \leq m$ und $-u^2 \equiv d \pmod{4m}$ bestimmen. ●

Der folgende Hilfssatz sagt, wann zwei Vektoren zur gleichen Bahn gehören können.

37. HILFSSATZ: Sei $L = \mathbb{Z}v_0 \oplus \mathbb{Z}v_1$, $v, v' \in L$,
 $q(v) = q(v')$, $v = v_1$, $v' = v_1 + x'v_0$, $x, x' \in \mathbb{Z}$, $x \neq x'$,
 Dann gibt es ein $u \in O(L)$ mit $uv = v'$.

Beweis:

Falls $v = v'$, wähle $u = \text{id}_L$.

Falls $v = v_1 + xv_0$, $v' = v_1 + x'v_0$, $x, x' \in \mathbb{Z}$, $x \neq x'$,
 so folgt

$$q(v_1) + x^2q(v_0) + xb(v_0, v_1) = q(v_1) + x'^2q(v_0) + x'b(v_0, v_1),$$

$$0 = (x^2 - x'^2)q(v_0) + (x - x')b(v_0, v_1),$$

$$q(v_0)(x + x') = -b(v_0, v_1), \quad q(v_0) \mid b(v_0, v_1).$$

Wäre $q(v_0) = 0$, so $b(v_0, v_1) = 0$ und L nicht regulär.

Die Spiegelung u , $u(w) := w - \frac{b(w, v_0)}{q(v_0)} v_0$ erfüllt

$uv_0, uv_1 \in L$, d.h. $u \in O(L)$ und $uv = v'$ ●

38. LEMMA: Sei L primitives binäres $\mathbb{Z}$ -Gitter, dL Diskriminante.

Dann gibt es unendlich viele $p \in \mathbb{P}$ mit

$$L \supseteq p.$$

Beweis: siehe (Web).

(Man kann auch von der Tatsache ausgehen, daß es unendlich viele Primideale ersten Grades in jeder (engeren) Idealklasse mod f von $\mathcal{O}_K$ gibt (s. N,S.94 u. Cor.7, S.325). Diese Eigenschaft läßt sich auf die engeren Idealklassen von Gittern K , $\mathcal{O}_K = \mathcal{O}_f$, übertragen, indem u.a. die Beziehung

$K = (\sigma_K, K) \cap \sigma_f$ für die zu f teilerfremden Gitter K ,
 $\sigma_K = \sigma_f$ bewiesen wird.

Zu gegebenem L gibt es ein L' auf V_0 mit $\text{prim } L' \cong L$.
 Sei $\mathfrak{g}$ ein Primideal von σ_L in der engeren Klasse von L' , d.h. $L' \cdot \mathfrak{g} = \alpha \sigma_L, \alpha \in L'$. Wenn $N \mathfrak{g} = p$, so folgt

$$\frac{N(\alpha)}{N\sigma_L} = \frac{N(\alpha)}{NL} = N\mathfrak{g} = p \in \mathbb{P}, \text{ d.h. } \text{prim } L' \rightarrow p. \quad \bullet$$

39. SATZ: Sei L primitives binäres $\mathbb{Z}\mathbb{Z}$ -Gitter, $d = dL$
 Diskriminante.

Dann sind folgende Aussagen äquivalent:

- a) $c(L) = 1$
- b) Falls $n \in \mathbb{Z}$, $|n| > 1$, $\text{ggT}(n, d) = 1$, $L \rightarrow n$ und
 nur eine Darstellung von n durch $L \bmod O(L)$
 existiert, so ist

$$|n| \in \mathbb{P} \quad .$$

Beweis:

b) $\Rightarrow$ a): Benutzt wird Hilfssatz 35 d). Sei dazu
 $\text{cls}^+ L = g_1 \cdot g_2$, $g_i = \text{cls}^+ G_i \in K^+(d)$. Nach Lemma 38
 gibt es $p_i \in \mathbb{Z}$, $|p_i| \in \mathbb{P}$ mit $|p_1| \neq |p_2|$,
 $\text{ggT}(p_1 p_2, d) = 1$ und $G_i \rightarrow p_i$, $i = 1, 2$. Nach 31 a)
 zeigt $L \rightarrow p_1 \cdot p_2 =: n$. Für $\text{cls}^+ L' := g_1^{-1} \cdot g_2$ folgt
 aus $\text{cls } G_1 = g_1 \vee g_1^{-1}$ ebenso $L' \rightarrow p_1 \cdot p_2$.
 Nach Voraussetzung gibt es mindestens zwei Bahnen
 von Darstellungen $\bmod O(L)$ von n durch L . Da
 nach Hilfssatz 36 keine weiteren Bahnen ex-
 istieren, muß $L \cong L'$, d.h. $\text{cls}^+ L = \text{cls}^+ L'$ oder

$\text{cls}^+L = (\text{cls}^+L')^{-1}$ gelten.

Dies bedeutet $g_1 \cdot g_2 = g_1^{-1} \cdot g_2$ oder $g_1 \cdot g_2 = g_1 \cdot g_2^{-1}$,

somit $g_1 = g_1^{-1}$ oder $g_2 = g_2^{-1}$, d.h.

$g_1 \in A$ oder $g_2 \in A$.

a) $\Rightarrow$ b): Sei $c(L) = 1$ und $n \in \mathbb{Z}$ mit den Voraussetzungen von b).

Dann wird nach Lemma 30 n nur von $\text{cls } L$ dargestellt, und zwar - nach Voraussetzung - nur einmal modulo $O(L)$. Somit sind alle Darstellungen primitiv. $|n| > 1$, $\text{ggT}(n, d) = 1$ ergibt

$\mu = \mu(n) > 0$, also mit Hilfssatz 36

$2^{\mu-1} = 1$, $\mu = 1$. Somit ist $|n| = p^a$, $p \in \mathbb{P}$, $a \in \mathbb{N}$.

Ist $a \geq 2$, so folgt aus $p \nmid \Delta(d)$, daß mit $L = \mathbb{Z}v \oplus \mathbb{Z}w$, $q(v) = n$ auch

$K := \mathbb{Z}(\frac{1}{p}v) \oplus \mathbb{Z}(pw)$ ein primitives Gitter ist.

Nach Lemma 30 folgt $K \in \text{gen } L$, da $K \supseteq \frac{n}{p^2}$,

$dK = dL$. $c(L) = 1$ impliziert $L \supseteq \frac{n}{p^2}$, so daß eine nichtprimitive Darstellung von n durch L existiert.

Dieser Widerspruch zeigt $a = 1$, damit $|n| \in \mathbb{P}$ ●

40. BEMERKUNG: Bedingung b) aus Satz 39 wurde von Euler im wesentlichen zur Definition einer "formula idonea" L benutzt. Allerdings betrachtete er nur positive quadratische Formen $ax^2 + by^2$, $\text{ggT}(a, b) = 1$, d.h. Gitter L mit Orthogonalbasis. $a \cdot b$ hieß "numerus idoneus", geeignet zum Auffinden von Primzahlen. Satz 39 zeigt, daß bei Untersuchung allgemeinerer "formulae idoneae" (s. Satz 39 b)) der weitere Klassenbegriff $c(L)$ angemessener ist als $c^+(L)$.

41. HILFSSATZ: Sei $d > 0$ eine Diskriminante.

Dann wird jede engere Klasse positiv-definiten prim.

$\mathbb{Z}$ -Gitter mit Diskriminante d durch genau eine (sogenannte reduzierte) Form (a,b,c) repräsentiert

mit $-a < b \leq a \leq c$

$b > 0$, falls $a = c$

$d = 4ac - b^2$, $\text{ggT}(a,b,c) = 1$.

Beweis: (s. z.B. J, Th. 76, S. 171) ●

42. SATZ: Sei $L \cong (a,b,c)$ primitiv und positiv-definit,
 $d = dL = \Delta(d) \cdot f^2$, $f \in \mathbb{N}$.

i) Aus $c(L) = 1$ folgt

E: Es gibt für $n = ax^2 + bx + c$, $x \in \mathbb{Z}$, $n \cdot a \leq d$,
 $\text{ggT}(n,f) = 1$ nur folgende Möglichkeiten:

a) $n = a$

b) $n \mid d$

c) $n = p \cdot d_0$ für $p \in \mathbb{P}$, $p \nmid d$, $d_0 \mid \Delta(d)$

d) $n = p^2 a$ und $a = p^i d_0$, $i \in \mathbb{N}_0$, $d_0 \mid \Delta(d)$,
 $(i \leq 1, \text{ falls } a = \min L := \min \{q(v) \mid 0 \neq v \in L\})$.

ii) Falls $a = f = 1$, so ist E äquivalent mit $c(L) = 1$.

Beweis:

i) Sei $L = \mathbb{Z}v_0 \oplus \mathbb{Z}v_1$, $q(v_0) = a$, $q(v_1) = c$, $b(v_0, v_1) = b$,

also $n = ax_0^2 + bx_0 + c = q(x_0 v_0 + 1 v_1)$. Nehmen wir an,

n habe eine weitere primitive Darstellung

$n = q(xv_0 + yv_1)$, $x, y \in \mathbb{Z}$. Eine quadratische

Ergänzung zeigt $4na = (2ax + by)^2 + dy^2$.

Falls $|y| \geq 2$, so ist $na \geq d$, also nach Voraussetzung $na = d$, $n|d$; ansonsten ist $|y| \leq 1$.

$y = 0$ ergibt wegen der Primitivität $x^2 = 1$ und $n = a$.

Sei nun $na \neq d$ und $n \neq a$.

Dann gilt für alle primitiven Darstellungen $y = \pm 1$.

Solche Darstellungen liegen nach Hilfssatz 37 alle in einer Bahn modulo $O(L)$. Da $\text{gen } L = \text{cls. } L$, $(n, f) = 1$, gilt entweder $\mu = \# \{ p \in \mathbb{P} | p|n, p \nmid d \} = 0$ oder es gibt nach Hilfssatz 36 $2^{\mu-1}$ primitive Darstellungsbahnen von $L \bmod O(L)$. Auf jeden Fall ist also $\mu \leq 1$,

d.h. $n = p^j \prod q_i$, $j \geq 0$, $q_i \in \mathbb{P}$, $q_i | d$, $p \in \mathbb{P}$, $p \nmid d$. Da $(n, f) = 1$, folgt sogar $q_i | \Delta = \Delta(d)$.

Nehmen wir an, es gilt $q^2 | n$ für ein $q = q_i$. Da n

primitiv dargestellt wird, gibt es $b, c \in \mathbb{Z}$, so daß

$d = 4nc - b^2$ gilt. $q|d$ ergibt $q^2 | b^2$, $q^2 | d$ und

$q^2 | \Delta$, da $(n, f) = 1$. Da Δ eine FD, bliebe nur $q = 2$; aber auch dies führt zum Widerspruch:

$\Delta \equiv d f^{-2} \equiv -(b f^{-1})^2 \pmod{16}$, aber $\Delta \not\equiv 0, -4 \pmod{16}$.

Damit hat n also die Gestalt $n = p^j d_0$, $d_0 | \Delta$.

Falls $j \leq 1$, folgen b) und c).

$j \geq 2$ impliziert $\frac{n}{p^2} = p^{j-2} d_0 \in L$, wie im Beweis von Satz 39 gezeigt, d.h.

$$\frac{n}{p^2} = q(xv_0 + yv_1) \quad \text{für } x, y \in \mathbb{Z}$$

$$n = q(pxv_0 + pyv_1).$$

$y \neq 0$ ergäbe mit $|py| \geq p \geq 2$ einen Widerspruch zur Abschätzung von n , so daß mit $y = 0$, $x = \pm 1$

$n = a \cdot p^2$, $a = p^{j-2} d_0$ folgt.

Würde $p^2 | a$ gelten, so ergäbe sich wie eben,

$\frac{n}{p_+} = \frac{a}{p_+} \in L$. Dann muß $a \neq \min L$ sein.

ii) Sei $L = (1, b, c)$, und es gelte "E". (A, B, C) sei eine nach Hilfssatz 41 reduzierte Form.

Da $4AC = B^2 + d$, $B \equiv d \equiv b \pmod{2}$, gibt es ein $x \in \mathbb{Z}$ mit $B = 2x + b$, d.h. $n := AC = x^2 + bx + c$.

Die Reduktionsbedingungen ergeben

$$d = 4AC - B^2 \geq 4AC - AC = 3AC, \text{ also } n \leq \frac{d}{3} < d.$$

Da auch $(n, f) = 1$, bleiben nach "E" für n die Möglichkeiten

$$n|d \text{ oder } n = p \cdot d_0, p \in \mathbb{P}, d_0|d \text{ oder } n = p^2.$$

In den ersten beiden Fällen folgt $A|d$ oder $C|d$, so daß (A, B, C) nach Lemma 34 c) ambig ist.

Im letzten Fall bleibt nur $(A, B, C) = (1, B, p^2)$ oder (p, B, p) , beides offensichtlich ambige Formen.

Insgesamt gibt es nur ambige Klassen, so daß $c(L) = c^+(d) = [K^+(d):A] = 1$ ●

43. BEMERKUNG: Es gilt nicht immer " $E \Rightarrow c(L) = 1$ "; dies ist leicht zu erkennen, wenn man ein Gitter L mit $c(L) > 1$ und $a \geq d$ wählt.

Aber sogar im Fall $a = \min L$ zeigt das Beispiel $L = (4, 3, 4)$, $dL = 55$, daß zwar "E" erfüllt ist, aber dennoch $c(L) > 1$ gilt (vgl. Tabelle, Kap. VI).
 $n = n(x) = 4x^2 + 3x + 4$, $4n \leq 55$ ist gleichbedeutend mit $|x| \leq 1$; $n(0) = 4$, $n(1) = 11$, $n(-1) = 5$.

B. Angenehme Gitter

44. DEFINITION: Sei L positiv-definites $\mathbb{Z}$ -Gitter.

L heißt angenehm, falls ein $N \in \mathbb{N}$ existiert, so daß für alle $n \gg N$ gilt:

$$L \ni n, \text{ falls } L_p \ni n \text{ für alle } p \in \mathbb{P}.$$

45. BEMERKUNG: Wie Satz 3 zeigt, sind einklassige Geschlechter angenehm. Andererseits gibt es aber auch angenehme Gitter L mit $c(L) > 1$ (vgl. W4).

46. LEMMA: Seien (L_i, q_i) primitive positive binäre $\mathbb{Z}$ -Gitter, $dL_i = d$, $i=1,2$. Es gelte für alle bis auf endlich viele $n \in \mathbb{N}$:

$$n \in q_2(L_2), \text{ falls } n \in q_1(L_1).$$

Dann ist

$$L_1 \cong L_2.$$

Beweis:

Nach Lemma 38 existiert ein $2 \nmid p \in \mathbb{P}$ mit $L_1 \ni p \in L_2$, also $L_1 \cong (p, b_1, c_1)$, $L_2 \cong (p, b_2, c_2)$, $b_i, c_i \in \mathbb{Z}$.

Aus $dL_1 = dL_2$ folgt $b_1^2 \equiv b_2^2 \pmod{4p}$, somit

$b_1 \equiv \pm b_2 \pmod{2p}$. Falls nötig, kann b_1 modulo $2p$ reduziert und b_1 durch $-b_1$ ersetzt werden, ohne daß sich die Klasse von L_1 verändert, so daß o.E. $b_1 = b_2$.

Dies ergibt $c_1 = c_2$ und $L_1 \cong L_2$ •

47. SATZ: Sei L binär, primitiv und positiv-definit.

Dann ist L genau dann angenehm, wenn $c(L) = 1$.

Beweis:

Sei L angenehm, $L' \in \text{gen } L$. Für hinreichend große $n \in \mathbb{N}$ mit $L' \not\supseteq n$ folgt $L'_p \not\supseteq n$, $L_p \supseteq n$ für alle $p \in \mathbb{P}$ und $L \supseteq n$. Lemma 46 beweist nun $L' \cong L$, also $c(L) = 1$ ●

C. Kongruenzbedingungen für einklassige Geschlechter

48. LEMMA: Sei $L \cong (a, b, c)$, $a, b, c \in \mathbb{Z}$ primitiv und positiv-definit.

Dann gilt:

a) Falls (a, b, c) reduziert, so ist L genau dann nichtambig, wenn $0 < |b| < a < c$.

b) Falls $a \nmid dL$ und

$$a^2 < \begin{cases} dL & , \text{ falls } 2^3 \parallel dL \\ \frac{dL}{4} & \text{sonst} \end{cases} ,$$

so ist L nichtambig.

Beweis:

a) Falls $b = 0$ oder $|b| = a$ oder $c = a$, so ist offensichtlich L ambig.

Falls $0 < |b| < a < c$, so gibt es zwei im weiteren, aber nicht im engeren Sinn isometrische reduzierte Formen (a, b, c) und $(a, -b, c)$.

b) Wäre L ambig, so gäbe es nach Lemma 34 ein $g \mid d = dL$ mit $L \cong (g, 0, \frac{d}{g})$, $g^2 \leq \frac{d}{4}$, oder $L \cong (g, g, \frac{d+g^2}{4g})$.

Im ersten Fall gibt es $x, y \in \mathbb{Z}$, $ggT(x, y) = 1$ mit
 $a = gx^2 + \frac{d}{4g} y^2$, da $a \in L$.

$y = 0$ ergäbe $a = g$, $a|d$ und den Widerspruch zu
 $a \nmid d$; analog betrachtet man $x = 0$.

Also gilt $a \geq g + \frac{d}{4g}$.

Für jedes $0 < r \in \mathbb{R}$ ist die Funktion $f(x) = \frac{r}{x} + x$
auf $0 < x \leq \sqrt{r}$ monoton fallend und $\min_{x>0} f = 2\sqrt{r}$.

Es folgt also $a \geq 2\sqrt{\frac{d}{4}} = \sqrt{d}$ im Widerspruch zur
Voraussetzung.

Im zweiten Fall, der nach Lemma 34 bei $2^3 \nmid d$ nicht
auftritt, ist

$$a = gx^2 + gxy + \frac{d+g^2}{4g} y^2 = g(x + \frac{1}{2}y)^2 + \frac{d}{4g} y^2,$$

wobei $ggT(x, y) = 1$.

$y = 0$ ergäbe den Widerspruch $a = g|d$. Wäre $y = -2x$, so

$x \nmid ggT(x, y) = 1$, d.h. $|y| = 2$, $a = \frac{d}{g}|d$.

Also ist hier $4a \geq g + \frac{d}{g} \geq 2\sqrt{d}$ im Widerspruch zur
Voraussetzung. ●

49. SATZ: Sei $d > 0$ eine binäre Diskriminante, $p \in \mathbb{P}$

mit $\left(\frac{-d}{p}\right) = 1$ (d.h. $-d \equiv 1 \pmod{8}$ für $p = 2$),

$$M := \begin{cases} d & , \text{ falls } 2^3 \nmid d \\ \frac{d}{4} & \text{sonst} \end{cases}.$$

Dann gilt:

a) Falls $p^2 \leq M$, so ist $c^+(d) > 1$.

b) Falls $p^4 \leq M$, so ist $c^+(d) > 2$.

Beweis:

- a) Da d eine Diskriminante und $\left(\frac{-d}{p}\right) = 1$, so zeigt man leicht, daß $b, c \in \mathbb{Z}$ existieren mit $d = 4pc - b^2$, $ggT(p, b, c) = 1$. Dann ist $L \cong (p, b, c)$ nach Lemma 48 nichtambig, so daß $c^+(d) = c^+(L) > 1$.
- b) Sei L wie in a) konstruiert. Da $L \supset p$, gibt es nach Lemma 31 ein Gitter $L' \in (cls^+L)^2 \in K^+(d)$ mit $L' \not\supset p^2$. Falls $L' \supset p^2$, so zeigt Lemma 48, daß L' nichtambig, d.h. $(cls^+L)^2 \notin A$. Dies impliziert nach Lemma 35 $c(L) > 1$, also $c^+(d) > 2$.
- Falls die Darstellung $L' \not\supset p^2$ nicht primitiv, so gilt $L' \supset 1$. Daraus folgt leicht $cls^+L' = 1 \in K^+(d)$, $(cls^+L)^2 = 1$, so daß L ambig wäre. ●

50. BEMERKUNG:

- a) Satz 49 a) erscheint schon in der Literatur, jedoch wurde M hier mehrmals falsch angegeben (vgl. SW, 8 d), S. 560; GRD, A c), S. 298; dazu als Gegenbeispiel u.a. $d = 187$, $p=7$).
- b) Um Satz 49 b) auf andere Art zu beweisen, kann man direkt eine nichtambige reduzierte Form L konstruieren, die p^2 als Minimum hat. Nun läßt sich unter Verwendung von Satz 39 zeigen, daß $p^2 \in \mathbb{P}$ wäre, wenn $c(L) = 1$, denn es gilt:
- Das Minimum eines positiven binären $\mathbb{Z}$ -Gitters L wird modulo $O(L)$ nur einmal dargestellt. Hierbei ist nur zu beachten, daß zwei linear unabhängige Minimumvektoren nach (vdW, S. 278 ff) eine Basis von L bilden.
- c) Da bei einer reduzierten Form $(a, b, c) = L$ $a = \min L$, findet man mit der obigen Bemerkung über das Minimum und mit Hilfe von Satz 39

schnell weitere Bedingungen folgender Art:

Falls $c(L) = 1$, $d = dL$, so enthält $\frac{d+b}{4}^2$,
 $b \equiv d \pmod{2}$ für "kleines" b "wenige" zu d
 teilerfremde Primfaktoren.

Solche Aussagen wurden bereits von N.Hall
 (s. H, S. 86) für den Fall $c^+(d) = 1$ angegeben.

D. Summen von drei Quadraten

51. LEMMA: Sei L positiv-definites ternäres $\mathbb{Z}$ -Gitter
 mit $c(L) = 1$, $n \in \mathbb{N}$, $\langle 2n \rangle \cong A \subseteq L$, A direkter
 Summand in L , $m = \left(\frac{dL}{sL}\right)_2$ und $K_1, \dots, K_l \subseteq L$ direkte
 binäre Summanden von L .

Für jede primitive Darstellung $v \in L$, $q(v) = n$
 gelte $v \in K_i$ modulo $O(L)$ für ein $i \in \{1, \dots, l\}$.

Dann gilt:

$$c(L, A, m, 1) \leq \sum_{K_i \supseteq A} c_{K_i},$$

wobei c_K die Anzahl der $y \in \{0, \dots, \left[\frac{dK}{2(sL)^2}\right]\}$ mit

$$\frac{2ndL}{(sL)^4} \equiv -y^2 \pmod{\frac{dK}{(sL)^2}};$$

$[x]$ ist dabei die größte ganze Zahl $z \leq x$.

Beweis:

Nach Satz 17 läßt sich $c(L, A, m, t)$ durch C abschätzen.
 Dies soll im vorliegenden Fall genauer untersucht
 werden.

Nach Formel (4) ist $c(L, A, m, t) \leq \sum_{K_i \supseteq A} g(L, K_i)$.

Sei nun $K := K_i$.

Da $t = 1$, $m = \frac{dL}{(sL)^2}$, kann nach Bemerkung 9 $e = 1$

gewählt werden, so daß mit Lemma 8

$$(L, N, m, t) = mL^{\#} \cap (QN)^{\perp}$$

für jeden direkten Summanden N von L .

Für $N = K$ ist $\text{rang}(L, K, m, t) = 1$. Aus Lemma 10 folgt

$$d(L, K, m, t) = d(m(L^{\#} \cap (QK)^{\perp}) = m^2 \frac{dK}{dL} = \frac{dK}{(sL)^4}, \quad \text{d.h.}$$

$$(7) \quad (L, K, m, t) \cong \left\langle \frac{dK}{(sL)^4} \right\rangle =: B \quad .$$

Für $N = A \cong \langle 2n \rangle$ ist $\text{rang}(L, A, m, t) = 2$ und

$$(8) \quad d(L, A, m, t) = m^4 \frac{dA}{dL} = \frac{2ndL^3}{(sL)^8} \quad .$$

Nach spezieller Wahl von m, t und e wird $g(L, K)$ abgeschätzt durch die Anzahl der reduzierten Vertreter $y_1, \dots, y_s \in \mathbb{Z}$ der Restklassen modulo B , die zusätzlich $y_i \not\equiv \pm y_j \pmod{B}$ für $i \neq j$ erfüllen (s. Beweis Satz 7). Außerdem gilt für diese y_i nach Konstruktion (s. Formel (5)) $m|y_i$ und nach Formel (6) $m|b(w_{U^1}, w_{U^1})$ also

$$d(L, A, m, t) \equiv -y_i^2 \pmod{m \cdot \det B} .$$

Sei $y_i^! \in \mathbb{Z}$, $y_i^! = \frac{y_i}{m}$.

Setzt man in die Kongruenz die oben berechneten Ausdrücke ein, so folgt

$$\frac{2n(dL)^3}{(sL)^8} \equiv -y_i^2 \pmod{\frac{(dL)^2 dK}{(sL)^6}}$$

$$\frac{2n(dL)^3}{(sL)^8} \equiv -y_i^{!2} \frac{dL^2}{(sL)^4} \pmod{\frac{(dL)^2 dK}{(sL)^6}}$$

$$\frac{2n \cdot dL}{(sL)^4} \equiv -y_i^{!2} \pmod{\frac{dK}{(sL)^2}}$$

Die reduzierten Vertreter $y_i^!$ der Klassen $\frac{B}{m}$,

$\frac{B}{m} = \frac{dK}{(sL)^2}$ mit $y_i^! \not\equiv \pm y_j^! \pmod{\frac{B}{m}}$ für $i \neq j$ sind:

$\{ 0, 1, \dots, [\frac{dK}{2(sL)^2}] \}$.

Zusammen mit der letzten Kongruenz gilt $g(L, K) \leq c_K$.

Daraus folgt die Behauptung ●

52. HILFSSATZ: Sei $E_3 := \mathbb{Z}e_1 \perp \mathbb{Z}e_1 \perp \mathbb{Z}e_3$, $q(e_i) = 1$

und $n \in \mathbb{N}$, $n \subsetneq E_3$, d.h. $n = x_1^2 + x_2^2 + x_3^2$,

$x_i \in \mathbb{Z}$, $i = 1, 2, 3$.

Dann gilt:

a) $4|n$ genau dann, wenn $2|x_i$ für $i = 1, 2, 3$.

b) $4 \nmid n$ genau dann, wenn $E_3 \supsetneq n$.

Beweis:

a) Dies folgt durch Kongruenzbetrachtung modulo 8.

b) Es gelte $4 \nmid n$. Für $p \in \mathbb{P}$ mit $p^2 \nmid n$ ist $(E_3)_p \supsetneq n$.

Falls $p^2|n$, also $p \nmid 4 = d(\mathbb{Z}e_1 \perp \mathbb{Z}e_2)$, so folgt nach (Kn, V, 14.7, S. 5) $(n-1) \subsetneq \mathbb{Z}_p e_1 \perp \mathbb{Z}_p e_2$.

Somit gilt $n \subsetneq (E_3)_p$ für alle $p \in \mathbb{P}$. Da bekanntlich nur eine primitive Klasse positiver ternärer $\mathbb{Z}$ -Gitter mit Diskriminante $dE_3 = 8$ existiert, folgt $c(E_3) = 1$, mit Satz 3 b) also $n \subsetneq E_3$ ●

53. BEISPIELE: Mit Hilfe von Lemma 51 kann man schnell konkrete Beispiele finden, die in Zusammenhang stehen mit einklassigen Geschlechtern.

Sei z.B. $L = E_3$, $n \in \mathbb{N}$, $4 \nmid n = x_1^2 + x_2^2 + x_3^2$, $x_i \in \mathbb{Z}$.

- a) Für jede solche Darstellung sei $x_i = 0$ für mindestens ein $i \in \{1, 2, 3\}$. Damit liegt jeder primitive Darstellungsvektor $v \in L$, $q(v) = n$, modulo $O(L)$ in $K_1 = \mathbb{Z}e_1 \perp \mathbb{Z}e_2$.
Da $dK_1 = 4$, $sL = 2$, folgt $c_{K_1} = 1$ (vgl. Lemma 51).
- b) Falls für jede Darstellung von n $x_i = 0$ oder $x_i = x_j$, für gewisse $i \neq j$, $i, j \in \{1, 2, 3\}$, so liegt v modulo $O(L)$ in K_1 oder $K_2 = \mathbb{Z}e_1 \perp \mathbb{Z}(e_2 + e_3)$.
Da $dK_2 = 8$, folgt auch $c_{K_2} = 1$, so daß $(L, \mathbb{Z}v, m, t)$ ein weiteres Beispiel von besonderem Interesse ist.

54. BEMERKUNG:

- a) Die natürlichen Zahlen n aus 53 a) wurden bereits von Schinzel (Sch) charakterisiert. Im Gegensatz zu der vorliegenden Methode müssen allerdings dort Sätze über Darstellungsanzahlen benutzt werden.
- b) Im folgenden werden die n aus 53 b) näher untersucht. Da nach Hilfssatz 52 a) n genau dann Summe von drei paarweise verschiedenen positiven Quadraten ist, wenn dies für $4n$ zutrifft, sei nun o.E. $4 \nmid n$.

55. SATZ: Sei $n \in \mathbb{N}$, $4 \nmid n$.

n ist genau dann Summe dreier positiver, paarweise verschiedener, teilerfremder, ganzzahliger Quadrate, wenn

- i) $n \not\equiv 0, 4, 7 \pmod{8}$ und

ii) 1) Es gibt ein $p \in \mathbb{P}$, $p \equiv 7 \pmod{8}$ mit $p|n$.

oder

2) Es gibt $p_1, p_2 \in \mathbb{P}$, $p_1 \equiv 3$, $p_2 \equiv 5 \pmod{8}$
mit $p_1 p_2 | n$.

oder

3) Es gibt ein $p \in \mathbb{P}$, $p \equiv 3$ oder $5 \pmod{8}$,
 $p|n \not\equiv 3 \pmod{8}$ und $c^+(4n) > 1$.

oder

4) Für alle $2 \neq p \in \mathbb{P}$ mit $p|n$ gilt $p \equiv 1 \pmod{8}$
und $c^+(4n) > 2$.

oder

5) $n \equiv 3 \pmod{8}$ und $c^+(n) > 1$.

Dabei ist für $n > 2$ im Fall 4) $c^+(4n) > 2$
genau dann, wenn $c^+(4n) \neq 2$.

Beweis:

Falls $4 \nmid n$, ist $n \subseteq E_3 =: L$ bekanntlich gleichbe-
deutend mit i). Sei nun generell $n \subseteq L$ vorausgesetzt.
Nach Hilfssatz 52 gilt auch $n \subseteq L$.

a) Sei $n \subseteq L$, aber jedes primitive $v \in L$ mit $q(v) = n$
liege $\text{mod } \mathcal{O}(L)$ in $K_1 = \mathbb{Z}e_1 \perp \mathbb{Z}e_2$ oder
 $K_2 = \mathbb{Z}e_1 \perp \mathbb{Z}(e_2 + e_3)$.

Hilfssatz 52 zeigt die Existenz eines primitiven v
mit $q(v) = n$.

Für ein solch primitives v , $v \in K_i$ sei $G_i = (L, \mathbb{Z}v, 2, 1)$.
Dann ist nach Lemma 8 $G_i = (L, K_i, 2, 1) \oplus \mathbb{Z}w$ für ein
 $w \in L$. Die Formeln (7) und (8) ergeben $(L, K_2, 2, 1) \cong \langle 4 \rangle$,
 $(L, K_1, 2, 1) \cong \langle 2 \rangle$, $dG_i = 4n$, so daß $G_i \cong (1, b_i, x_i)$,

$G_2 \cong (2, b_2, x_2)$ mit $2|b_i$, da $G_i \subseteq L$ und somit $2|sG_i$, $i=1,2$.

Durch Reduktion von $b_1 \bmod 2$ und $b_2 \bmod 4$ ergibt sich

$$G_1 \cong (1, 0, n)$$

und

$$G_2 \cong \begin{cases} (2, 0, \frac{n}{2}) & , \text{ falls } 2|n \\ (2, 2, \frac{n+1}{2}) & , \text{ falls } 2 \nmid n \end{cases} .$$

Sei nun v fest gewählt. Dann besteht nach Satz 14 gen $(L, \mathbb{Z}v, 2, 1)$ nur aus Gitterklassen G_1 oder G_2 .

Falls $n \equiv 3 \bmod 4$, gilt offensichtlich $n \notin K_1$, so daß nur der G_2 -Typ auftritt, also

$$c(2, 2, \frac{n+1}{2}) = c(1, 1, \frac{n+1}{4}) = 1 ; \text{ anders gesagt } c^+(n) = 1.$$

Falls $p|n$ für ein $p \in \mathbb{P}$, $p \equiv 3$ oder $5 \bmod 8$, so gilt $n \notin K_1$ bzw. $n \notin K_2$, so daß $c(1, 0, n) = 1$

$$\text{oder } c(2, 0, \frac{n}{2}) = 1 \text{ oder } c(2, 2, \frac{n+1}{2}) = 1.$$

Da es sich hier um ambige Klassen handelt, kann dies für $n \not\equiv 3 \bmod 4$ mit $c^+(4n) = 1$ ausgedrückt werden.

Falls schließlich für alle $2 \neq p \in \mathbb{P}$ mit $p|n$, $p \equiv 1 \bmod 8$ folgt, so gilt

$$\text{gen } (1, 0, n) = \begin{cases} \{\text{cls}(1, 0, n), \text{cls}(2, 0, \frac{n}{2})\} & \text{für } n \equiv 2 \bmod 4 \\ \{\text{cls}(1, 0, n), \text{cls}(2, 2, \frac{n+1}{2})\} & \text{für } n \equiv 1 \bmod 4 \end{cases}$$

Beide Klassen sind wirklich in einem Geschlecht:

Für $p \nmid 4n$ sind alle primitiven Gitter $\mathbb{Z}_p$ -isometrisch;

für $2 \neq p|4n$ beachte, daß $(\frac{2}{p}) = 1$, d.h. $2 \in \mathbb{Z}_p^{*2}$

$$\text{und } (2, 2, \frac{n+1}{2})_p \cong (1, 0, n)_p \cong (2, 0, \frac{n}{2})_p ;$$

falls $p = 2$, $n \equiv 2 \pmod{4}$ ist $\frac{n}{2} \in \mathbb{Z}_2^{*,2}$;

für $p = 2$, $n \equiv 1 \pmod{4}$ ist $n \in \mathbb{Z}_2^{*,2}$, also

$(n, 0, 1)_2 \cong (1, 0, 1)_2 \ni 2$ und damit

$(n, 0, 1)_2 \cong (2, 2, \frac{n+1}{2})_2$.

Da die Formen - falls $n > 2$ - reduziert und verschieden sind, gilt hier also $c^+(4n) = 2$;

$c^+(4n) = 1$ tritt unabhängig von den übrigen Voraussetzungen nur für $n \leq 2$ auf.

- b) Zur Umkehrung sei zunächst bemerkt, daß für $p|n$, $p \in \mathbb{P}$ aus dem quadratischen Reziprozitätsgesetz im Falle $p \equiv 3, 7 \pmod{8}$ $n \notin K_1$, im Falle $p \equiv 5, 7 \pmod{8}$ $n \notin K_2$ folgt.

Nehmen wir nun an, es gelte weder 1) noch 2).

Lokale Überlegungen und Satz 3 genügen, um zu zeigen, daß $n \subset K_1$ (bzw. $n \subset K_2$) gilt, falls $p \equiv 1, 5 \pmod{8}$ (bzw. $p \equiv 1, 3 \pmod{8}$) für alle $2 \neq p \in \mathbb{P}$, $p|n$.

Sei $v \in L$ eine solche primitive Darstellung, $q(v) = n$ und v' eine beliebige primitive Darstellung von n . Dann gilt für die Injektion $(\mathbb{Z}v \rightarrow L) \in \text{gen}(\mathbb{Z}v' \rightarrow L)$: Die $\mathbb{Z}_p$ -Isometrie, $p \neq 2$ gilt nach dem Fortsetzungssatz von Witt (Kn, I., Satz 3.4 a), S. 15), da L_p unimodular und $\mathbb{Z}_p v$ ein im Sinne von Kneser (Kn, I., S. 7-8) gutes Gitter ist.

Aber auch für $p = 2$ gibt es eine Isometrie $u \in O(L_2)$, $u(v') = v$: Falls $w \in L_2$, $4 \nmid q(w)$ oder $w \in 2L_2$,

$8 \nmid q(w)$, so gilt $\frac{b(x, w)}{q(w)} \in \mathbb{Z}_2$ für alle $x \in L_2$,

so daß die Spiegelung $s_w: x \mapsto x - \frac{b(x, w)}{q(w)} w \in O(L_2)$.

Sei $w := v - v'$. Falls $4 \nmid q(w)$ liefert $s_w(v') = v$ die Behauptung.

Sei nun $4|q(w)$, $n \not\equiv 3 \pmod{4}$. Dann erreicht man durch eventuelle Permutation der Koordinaten von v und v' bzgl. der Basis (e_1, e_2, e_3)

$$b(v, e_1 + e_2) \equiv b(v', e_1 + e_2) \equiv 2 \pmod{4}.$$

Für $e \in L_2, w' := v - s_e(v') = \frac{b(v', e)}{q(e)} e + w$ gilt

$$q(w') = \frac{b(v', e)b(v, e)}{q(e)} + q(w).$$

$e := e_1 + e_2$ ergibt $q(e) = 2, 4 \nmid q(w')$, so daß $s_e, s_{w'} \in O(L_2)$ und $s_{w'}(s_e(v')) = v$.

Für $4 \mid q(w)$, $n \equiv 3 \pmod{8}$ folgt $w = v - v' \in 2L_2$.

Falls $8 \nmid q(w)$, so ist $s_w \in O(L_2)$ und $s_w(v') = v$; falls $8 \mid q(w)$, wähle $e := e_1$, $q(e) = 1$ und $w' \in 2L_2$, $8 \nmid q(w')$. Damit liefert $s_{w'} \circ s_e$ die gesuchte Isometrie.

Satz 14 zeigt nun $(L, \mathbb{Z}v', 2, 1) \in \text{gen}(L, \mathbb{Z}v, 2, 1)$. Da $(L, \mathbb{Z}v, 2, 1) \cong G_i, i \in \{1, 2\}$, ergibt die Verneinung der Voraussetzungen 3) - 5), daß auch $(L, \mathbb{Z}v', 2, 1) \cong G_j, j \in \{1, 2\}$. Damit gibt es ein $z \in L \cap \mathbb{Q}v'^\perp$, $q(z) = 1$ oder 2 , womit $z = \pm e_i$ oder $\pm e_i \pm e_j, i \neq j$ folgt. Also ist $v' \in K_1$ oder $v' \in K_2$ modulo $O(L)$ •

56. SATZ: Sei $n \in \mathbb{N}, 4 \nmid n$.

Besitzt n eine Darstellung als Summe positiver paarweise verschiedener Quadrate, dann existiert auch eine derartige Darstellung mit teilerfremden Quadraten.

Beweis:

n habe eine Darstellung als Summe positiver paarweise verschiedener Quadrate; jede Darstellung dieser Art sei nicht primitiv. Dann folgt nach Satz 55, daß $p \equiv 1, 3 \pmod{8}$ für alle $p \in \mathbb{P}$, $2 \neq p \mid n$ gilt oder alle p erfüllen $p \equiv 1, 5 \pmod{8}$. Weiter gibt es ein $1 < c \in \mathbb{N}, 2 \nmid c$, so daß $\frac{n}{c}$ Summe paarweise verschiedener, positiver

teilerfremder Quadrate ist.

Sei zunächst $n \not\equiv 3 \pmod{8}$ und $p \in \mathbb{P}$, $p \nmid n$ mit $p \equiv 3, 5 \pmod{8}$. Satz 55 ergibt $c^+(4n) = 1$, also auch $c^+(\frac{4n}{c^2}) = 1$ nach Folgerung 32.

Gäbe es ein $p' \in \mathbb{P}$, $p' \equiv 3, 5 \pmod{8}$, $p' \nmid \frac{n}{c^2}$, so wäre mit Satz 55 $c^+(\frac{4n}{c^2}) > 1$.

Also erfüllen alle $2 \nmid p \mid \frac{n}{c^2}$ die Bedingung $p \equiv 1 \pmod{8}$. Dann folgt aus Satz 55 der Widerspruch $c^+(\frac{4n}{c^2}) > 2$.

Ebenso führt $p \equiv 1 \pmod{8}$ für alle $2 \nmid p \mid n$, $p \in \mathbb{P}$ mit Hilfe von Satz 55 sowohl zu $c^+(4n) \leq 2$ und damit auch zu $c^+(\frac{4n}{c^2}) \leq 2$, als auch zu $c^+(\frac{4n}{c^2}) > 2$.

Sei nun $n \equiv 3 \pmod{8}$. Dann ist auch $\frac{n}{c^2} \equiv 3 \pmod{8}$; Satz 55 und die Monotonie von c^+ liefern den Widerspruch ●

Satz 55 und die Monotonie der Klassenzahl c^+ lassen vermuten, daß quadratfreie n von besonderem Interesse sind.

57. SATZ: Sei $n \in \mathbb{N}$, $n \not\equiv 0, 4, 7 \pmod{8}$. n habe keine Darstellung als Summe paarweise verschiedener positiver Quadrate.

Dann ist n quadratfrei, es sei denn $n \in \{9, 18, 25, 27, 99\}$.

Beweis:

Sei $n \not\equiv 3 \pmod{8}$ und n nicht quadratfrei, d.h. $4n$ keine FD;
 $d := 4n = f^2 \Delta$, $\Delta = \Delta(d)$.

Falls $p \equiv 3, 5 \pmod{8}$ für ein $p \in \mathbb{P} \ni p|n$, so folgt
nach Satz 55 $c^+(d) = 1$.

Wenn $\Delta > 4$, so ergibt Satz 63, S. 58
und $n \not\equiv 0, 3, 4, 7 \pmod{8}$ $d \in \{3^2 \cdot 8, 3^2 \cdot 20\}$. $n = 3^2 \cdot 5$
entfällt wegen Satz 55, ii), 2).

Wenn $\Delta \leq 4$, so ergibt Satz 62, S. 55
 $d \in \{3^2 \cdot 4, 5^2 \cdot 4\}$.

Falls $p \equiv 1 \pmod{8}$ für alle $p \in \mathbb{P}$, $2 \neq p|n$, so
folgt nach Satz 55 $c^+(d) = 2$. Damit gilt $c^+(\Delta) \leq 2$.
Die Bedingungen an n zusammen mit Satz 63, S. 58
lassen hier kein weiteres d zu.

Sei nun $n \equiv 3 \pmod{8}$, $n = f^2 \Delta$, $\Delta = \Delta(n)$ und n
keine FD. Satz 55 zeigt $c^+(n) = 1$, $c^+(\Delta) = 1$.
Zusammen mit Satz 55, ii), 2) ergibt sich aus
 $n \in \{3^2 \cdot 11, 3^2 \cdot 3\}$ ●

58. KOROLLAR: Jedes ungerade Quadrat bis auf 1, 9 und
25 ist Summe dreier positiver, paarweise ver-
schiedener Quadrate.

59. SATZ: Sei $n \in \mathbb{N}$, $n \not\equiv 0, 4, 7 \pmod{8}$, $n \leq 10^7$, falls
 $n \equiv 3 \pmod{8}$ und $4n \leq 10^7$ sonst.

Dann ist n Summe dreier positiver, paarweise
verschiedener Quadrate, es sei denn

$n \in \{1, 2, 3, 5, 6, 9, 10, 11, 13, 17, 18, 19, 22, 25, 27, 33, 34,$
 $37, 43, 51, 57, 58, 67, 73, 82, 85, 97, 99, 102, 123, 130,$
 $163, 177, 187, 193, 267, 627, 697\}$.

Beweis:

Man suche in der Tabelle (S. 66) alle nach Satz 55 in Frage kommenden FD d. Zusammen mit Satz 57 folgt die Behauptung ●

Die Ergebnisse legen die Vermutung nahe, daß 697 die letzte Ausnahme ist.

60. BEMERKUNG: So wie das eben behandelte Problem lassen sich auch viele andere durch Lemma 51 mit einklassigen Geschlechtern in Verbindung bringen.

Ohne ausführlich zu werden, sei noch folgendes Beispiel erwähnt:

Die Zahlen $n \in E_3$, $n = x_1^2 + x_2^2 + x_3^2$, $0 \leq x_1 \leq x_2 \leq x_3$, für die der Abstand aufeinander folgender x_i immer gleich ist, führen zu einschränkenden Gittern $K = \mathbb{Z}(2e_1 + e_3) \oplus \mathbb{Z}(e_1 - e_3)$, $dK = 24$ und mit Lemma 51 auf einklassige Geschlechter. Genauer:

$$c(G) = 1, G = (6, 0, \frac{n}{6}), (6, 2, \frac{n+1}{6}), (6, 4, \frac{n+4}{6}), (6, 6, \frac{n+9}{6}),$$

je nachdem, ob $n \equiv 0, 5, 2, 3 \pmod{6}$.

Auch hier treten also Gitter mit $c^+(G) = 2$ auf.

V. REDUKTION AUF FUNDAMENTALDISKRIMINANTEN

61. LEMMA: Sei $d > 0$ eine binäre Diskriminante,
 $d = f^2 \Delta$, $f \in \mathbb{N}$, Δ FD, $t = \# \{ p \in \mathbb{P} \mid p \mid \Delta \}$,
 $u = \# \{ p \in \mathbb{P} \mid p \mid f, p \nmid \Delta \}$,

$$\bar{u} := \begin{cases} u - 1, & \text{falls i): } 2^1 \parallel f, 2 \nmid \Delta \\ u, & \text{falls ii): } (2 \nmid f) \text{ oder } (2^1 \parallel f, 2^2 \parallel \Delta) \text{ oder } (2^2 \parallel f, 2 \nmid \Delta). \\ u + 1, & \text{falls iii): } (2^1 \parallel f, 2^3 \parallel \Delta) \text{ oder } (2^2 \parallel f, 4 \mid \Delta) \text{ oder } (8 \mid f); \end{cases}$$

$$\bar{e} := \begin{cases} 1, & \text{falls } \Delta > 4 \text{ oder } (\Delta \in \{3, 4\}, f=1) \\ 2, & \text{falls } \Delta = 4, f > 1 \\ 3, & \text{falls } \Delta = 3, f > 1. \end{cases}$$

Weiter bezeichne $g(d)$ die Anzahl der Geschlechter in $K^+(d)$.

Dann gilt: a) $g(\Delta) = 2^{t-1}$

$$b) \quad g(d) = g(\Delta) \cdot 2^{\bar{u}}$$

$$c) \quad c^+(d) = c^+(\Delta) \cdot \frac{f}{2^{\bar{e}}} \prod_{p \mid f, p \nmid \Delta} \left(1 - \left(\frac{-\Delta}{p} \right) \frac{1}{p} \right).$$

Beweis:

b): Nach (J, Theorem 75, S. 170) gilt

$$g(d) = \begin{cases} 2^s, & \text{falls } 2 \nmid d, \frac{d}{4} \equiv 1 \pmod{4} \text{ oder } \frac{d}{4} \equiv 0 \pmod{8} \\ 2^{s-1}, & \text{sonst} \end{cases},$$

$$\text{wobei } s = \begin{cases} \#\{p \in \mathbb{P} \mid p \mid d\} & , \text{ falls } 2 \nmid d \\ \#\{p \in \mathbb{P} \mid p \mid \frac{d}{4}\} & , \text{ falls } 2 \mid d . \end{cases}$$

Dabei ist nur zu beachten, daß bei Jones die Diskriminante der vierte Teil unserer Diskriminante bedeutet.

Wenn $s' := \#\{p \in \mathbb{P} \mid p \mid d\}$, so gilt $s' = u + t$ und

$$g(d) = \begin{cases} 2^{s'-2} & , \text{ falls } 2^2 \parallel d, \frac{d}{4} \equiv 3 \pmod{4} \quad (i) \\ 2^s & , \text{ falls } 32 \mid d \quad (iii) \\ 2^{s-1} & \text{sonst} \quad (ii) . \end{cases}$$

a): Insbesondere gilt $g(\Delta) = 2^{t-1}$, da hier ii) und $u = 0$ eintreten.

c): Nach (L, Satz 214 u. Satz 209) gilt

$$h^+(d) = h^+(\Delta) \prod_{p \mid f} \left(1 - \left(\frac{-\Delta}{p}\right) \frac{1}{p}\right) . \quad (+)$$

Aus $c^+ = \frac{h^+}{g}$ und b) folgt die Behauptung ●

62. HILFSSATZ: Seien d, Δ und f wie in Lemma 61,

$$v = \frac{c^+(d)}{c^+(\Delta)} .$$

Dann gilt:

a) $\Delta = 3$:

$$\begin{aligned} v = (c^+(d)) = 1 & \Leftrightarrow f \in \{1, 2, 3, 4, 5, 7, 8\} \\ v = 2 & \Leftrightarrow f \in \{11, 13\} \end{aligned}$$

b) $\Delta = 4$:

$$V = (c^+(d)) = 1 \iff f \in \{1, 2, 3, 4, 5\}$$

$$V = 2 \iff f \in \{6, 7, 8, 10, 12, 15, 20\}$$

c) $\Delta > 4$:

$V = 1$ genau dann, wenn eine der folgenden Bedingungen erfüllt ist:

$$f = 1$$

$$f = 2 \quad \left(\frac{-\Delta}{2}\right) = 1$$

$$f = 6 \quad \left(\frac{-\Delta}{2}\right) = \left(\frac{-\Delta}{3}\right) = 1$$

$$f = 4 \quad \left(\frac{-\Delta}{2}\right) = 1$$

$$f = 12 \quad \left(\frac{-\Delta}{2}\right) = \left(\frac{-\Delta}{3}\right) = 1$$

$$f = 3 \quad \left(\frac{-\Delta}{3}\right) = 1$$

$$f = 2 \quad 2^3 \parallel \Delta$$

$$f = 6 \quad \left(\frac{-\Delta}{3}\right) = 1, 2^3 \parallel \Delta$$

$$f = 8 \quad \left(\frac{-\Delta}{2}\right) = 1$$

$$f = 24 \quad \left(\frac{-\Delta}{2}\right) = \left(\frac{-\Delta}{3}\right) = 1$$

$V = 2$ genau dann, wenn eine der folgenden Bedingungen erfüllt ist:

$$f = 6 \quad \left(\frac{-\Delta}{2}\right) = 1 = -\left(\frac{-\Delta}{3}\right)$$

$$f = 2 \quad 2^2 \parallel \Delta$$

$$f = 6 \quad \left(\frac{-\Delta}{3}\right) = 1, \quad 2^2 \parallel \Delta$$

$$f = 3 \quad \left(\frac{-\Delta}{3}\right) = -1$$

$$f = 5 \quad \left(\frac{-\Delta}{5}\right) = 1$$

$$f = 15 \quad \left(\frac{-\Delta}{5}\right) = \left(\frac{-\Delta}{3}\right) = 1$$

$$f = 12 \quad \left(\frac{-\Delta}{2}\right) = 1 = -\left(\frac{-\Delta}{3}\right)$$

$$f = 20 \quad \left(\frac{-\Delta}{2}\right) = 1 = \left(\frac{-\Delta}{5}\right)$$

$$f = 60 \quad \left(\frac{-\Delta}{2}\right) = \left(\frac{-\Delta}{3}\right) = \left(\frac{-\Delta}{5}\right) = 1$$

$$f = 4 \quad 4 \mid \Delta$$

$$f = 12 \quad \left(\frac{-\Delta}{3}\right) = 1, \quad 4 \mid \Delta$$

$$f = 6 \quad \left(\frac{-\Delta}{3}\right) = -1, \quad 2^3 \parallel \Delta$$

$$f = 10 \quad \left(\frac{-\Delta}{5}\right) = 1, \quad 2^3 \parallel \Delta$$

$$f = 30 \quad \left(\frac{-\Delta}{5}\right) = \left(\frac{-\Delta}{3}\right) = 1, \quad 2^3 \parallel \Delta$$

$$f = 16 \quad \left(\frac{-\Delta}{2}\right) = 1$$

$$f = 24 \quad \left(\frac{-\Delta}{2}\right) = 1 = -\left(\frac{-\Delta}{3}\right)$$

$$f = 48 \quad \left(\frac{-\Delta}{2}\right) = \left(\frac{-\Delta}{3}\right) = 1$$

Beweis:

$$\text{Sei } f_0 := \prod_{p \mid f, p \mid \Delta} p^i, \quad f_1 := \frac{f}{f_0}, \quad M := \frac{2f_1}{\prod_{p \mid f_1} p} \prod_{p \mid f_1} \frac{p - \left(\frac{-\Delta}{p}\right)}{2}.$$

Dann ist $\text{ggT}(f_0, f_1) = \text{ggT}(\Delta, f_1) = 1$, $u = \#\{p \in \mathbb{P} \mid p \mid f_1\}$,
 $M \in \mathbb{N}$.

Nach Lemma 61 gilt

$$\bar{e} \cdot V = \begin{cases} M \cdot f_0 & \text{im Falle i)} \\ \frac{M}{2} \cdot f_0 & \text{im Falle ii)} \\ \frac{M}{4} \cdot f_0 & \text{im Falle iii)} \end{cases} .$$

Sei $V \leq 2$. Dann ist auch f_0 nach oben beschränkt, da $M \in \mathbb{N}$. Zu festem f_0 ist $M \in \mathbb{N}$ durch V bestimmt.

$M \geq 2 \prod_{p|f_1} \frac{p-1}{2}$ zeigt nun, daß für $p|f_1$ nur gewisse $p \in \mathbb{P}$ in Frage kommen. $M \geq \frac{f_1}{\prod_{p|f_1} p}$ zeigt, daß diese p nur mit beschränkter Potenz in f_1 aufgehen.

Rechnen wir als Beispiel den Fall i), $\Delta > 4$ durch. Dann ist $V = M \cdot f_0$. Aus $V \leq 2$ folgt $f_0 \leq 2$. $f_0 = 2$ ergäbe $2|\Delta$ im Widerspruch zu i).

$f_0 = 1$ führt zu $M \leq 2$. Da $M \geq 4$, falls $p \geq 5$, $p|f_1$, kommt nur $p \in \{2, 3\}$ als Teiler von f_1 in Frage.

$\frac{f_1}{\prod_{p|f_1} p} \leq 2$ zeigt $f_1 \in \{2, 4, 6, 12\}$; aber $f_1 \in \{4, 12\}$

wird durch i) ausgeschlossen.

$f_1 = 2$ erzwingt nach Definition von M $(\frac{-\Delta}{2}) = 1$ und damit $V = M = 1$.

$f_1 = 6$ beläßt die Möglichkeiten $(\frac{-\Delta}{2}) = (\frac{-\Delta}{3}) = 1$, $V = 1$ und $(\frac{-\Delta}{2}) = 1 = -(\frac{-\Delta}{3})$, $V = 2$.

Analoge Betrachtungen für die weiteren Fälle be-
weisen den Hilfssatz ●

63. SATZ: Seien d, Δ , f wie in Lemma 61, $f > 1$, $\Delta > 4$,

$$M_1 := \{ 2^2 \cdot 7, 2^2 \cdot 15, 4^2 \cdot 7, 4^2 \cdot 15, 3^2 \cdot 8, 3^2 \cdot 11, 3^2 \cdot 20, 3^2 \cdot 35, 6^2 \cdot 8, 8^2 \cdot 7, 8^2 \cdot 15 \}$$

$$M_2 := \{ 6^2 \cdot 7, 6^2 \cdot 20, 5^2 \cdot 11, 5^2 \cdot 19, 5^2 \cdot 24, 5^2 \cdot 51, 5^2 \cdot 84, 5^2 \cdot 91, 15^2 \cdot 11, \\ 12^2 \cdot 7, 12^2 \cdot 8, 12^2 \cdot 20, 10^2 \cdot 24, 16^2 \cdot 7, 16^2 \cdot 15, 24^2 \cdot 7 \} .$$

$$M_3 := \{ 2^2 \cdot 39, 2^2 \cdot 55, 4^2 \cdot 39, 4^2 \cdot 55, 3^2 \cdot 56, 3^2 \cdot 68, 3^2 \cdot 260, 3^2 \cdot 308, \\ 3^2 \cdot 155, 3^2 \cdot 203, 3^2 \cdot 323, 6^2 \cdot 56, 8^2 \cdot 39, 8^2 \cdot 55 \} .$$

Dann gilt:

$$a_1) \quad c^+(d) = 1 \text{ für } d \in M_1 .$$

$$a_2) \text{ Falls } d \notin M_1, \quad c^+(\Delta) = 1, \text{ so folgt:}$$

$$c^+(d) = 1 \quad \Leftrightarrow \quad d = 2^2 \cdot \Delta, \quad 2^3 \nmid \Delta .$$

$$b_1) \quad c^+(d) = 2, \quad c^+(\Delta) = 1 \text{ für } d \in M_2 .$$

$$b_2) \text{ Falls } d \notin M_2, \quad c^+(\Delta) = 1, \text{ so folgt:}$$

$$\begin{aligned} c^+(d) = 2 \quad \Leftrightarrow \quad d = 3^2 \cdot \Delta, \quad \Delta \equiv 1 \pmod{3} \quad \text{oder} \\ d = 6^2 \cdot \Delta, \quad \Delta \equiv 1 \pmod{3}, 2^3 \nmid \Delta \quad \text{oder} \\ d = 2^2 \cdot \Delta, \quad 2^2 \nmid \Delta \quad \text{oder} \\ d = 4^2 \cdot \Delta, \quad 4 \mid \Delta \end{aligned}$$

$$c_1) \quad c^+(d) = c^+(\Delta) = 2 \text{ für } d \in M_3 .$$

$$c_2) \text{ Falls } d \notin M_3, \quad c^+(\Delta) = 2, \text{ so folgt:}$$

$$c^+(d) = 2 \quad \Leftrightarrow \quad d = 2^2 \cdot \Delta, \quad 2^3 \nmid \Delta .$$

Beweis:

Nach Satz 49 gilt $c^+(\Delta) > 1$ (bzw. $c^+(\Delta) > 2$), falls

$$\left(\frac{-\Delta}{2}\right) = 1, \quad \Delta \geq 16 \quad (\Delta \geq 64)$$

$$\left(\frac{-\Delta}{3}\right) = 1, \quad \Delta \geq 36 \quad (\Delta \geq 324)$$

$$\left(\frac{-\Delta}{5}\right) = 1, \quad \Delta \geq 100 \quad (\Delta \geq 2500) .$$

Nimmt man eine Klassenzahlentabelle zur Hand (BS, Tabelle 4, S. 457) und benutzt Lemma 61 a), so zeigt sich:

$$\begin{array}{ll}
 \Delta \in \{7, 15\} & \Leftrightarrow \left(\frac{-\Delta}{2}\right) = 1, c^+(\Delta) = 1 \\
 \Delta \in \{39, 55\} & \Leftrightarrow \left(\frac{-\Delta}{2}\right) = 1, c^+(\Delta) = 2 \\
 \Delta \in \{8, 11, 20, 35\} & \Leftrightarrow \left(\frac{-\Delta}{3}\right) = 1, c^+(\Delta) = 1 \\
 \Delta \in \{56, 68, 155, 203, \\
 \quad 260, 308, 323\} & \Leftrightarrow \left(\frac{-\Delta}{3}\right) = 1, c^+(\Delta) = 2 \\
 \Delta \in \{11, 19, 24, 51, 84, 91\} & \Leftrightarrow \left(\frac{-\Delta}{5}\right) = 1, c^+(\Delta) = 1 .
 \end{array}$$

Untersucht man daraufhin Hilfssatz 62 c), so folgt die Behauptung ●

Satz 63 a₂) wurde von Grosswald (GRÖ, Theorem 1, S. 297) bewiesen, allerdings unter falscher Angabe der Schranke $d > 315$ für die Ausnahmen der Äquivalenz in a₂).

Zusammen mit Hilfssatz 62 a), b) ist durch Satz 63 das Problem der Diskriminanten einklassiger Geschlechter vollständig auf Geschlechter mit Fundamentaldiskriminante zurückgeführt.

VI. NUMERISCHE ERGEBNISSE

64. SATZ: Sei $d \in \mathbb{D}$, $0 < \delta < \frac{1}{2}$, $\delta \in \mathbb{R}$.

Dann gibt es eine Schranke $S(\delta) \in \mathbb{R}$, so daß

$$c^+(d) > d^\delta \quad \text{für alle } d > S(\delta).$$

$S(\delta)$ ist nicht effektiv.

Beweis:

Siegel (S) bewies, daß für jedes $\varepsilon > 0$ $h^+(d) > d^{\frac{1}{2}-\varepsilon}$, falls d hinreichend groß ist. Mit Lemma 61, $t = \#\{p \in \mathbb{P} \mid p \mid d\}$ folgt für jedes $0 < \delta < \frac{1}{2}$
 $c^+(d) > \frac{d^\delta}{2^t}$ für große d .

Sei $\{p_1, p_2, \dots\} = \mathbb{P}$, $p_1 = 2$, $p_i < p_{i+1}$ für alle i
 und $P_t := \prod_{1 \leq i \leq t} p_i$.

Durch Induktion nach $r \in \mathbb{N}$ zeigt man leicht, daß zu jedem $r \in \mathbb{R}$, $r > 0$ ein t_0 existiert mit $r^t < P_t$ für alle $t \geq t_0$.

Sei $0 < \delta' < \frac{1}{2}$ gegeben und $\varepsilon > 0$ so, daß $\delta := \delta' + \varepsilon < \frac{1}{2}$.

Mit $r := 2^{\frac{1}{t}}$, $d \geq P_t$ folgt $c^+(d) > \frac{d^{\delta'}}{2^{\frac{\varepsilon}{t}}}$ für $t \leq t_0$

und $c^+(d) > \frac{d^{\delta'}}{2^{\frac{\varepsilon}{t}}} = \frac{d^{\varepsilon}}{2^{\frac{\varepsilon}{t}}} d^{\delta'} \geq \left(\frac{P_t}{r^t}\right)^{\varepsilon} d^{\delta'} > d^{\delta'}$, falls $t \geq t_0$.

Dies liefert die Behauptung ●

65. BEMERKUNG:

- a) Satz 64 zeigt, daß nur endlich viele $\mathbb{D}$ $d > 0$ mit $c^+(d) \leq 2$ existieren. Mit den Ergebnissen aus Kapitel V gibt es also nur endlich viele einklassige Geschlechter positiv-definiten primitiver binärer quadratischer Formen L (vgl. Ch u. B-Sch).

- b) G.L. Watson (W3, Theorem 1, S. 549) benutzte die Transformationen, die die Klassenzahl nicht erhöhen, um $c(L) > 1$ für $\text{rg } L > 10$, L positiv-definit zu beweisen.

Im definiten Fall gibt es immer nur endlich viele primitive Geschlechter L , $\text{rg } L > 1$, mit konstantem $c(L)$, wie man z.B. aus den allgemeinen Ergebnissen von H. Pfeuffer (P, Satz 4, S. 409) erkennt.

66. SATZ:

- a) Es gibt höchstens eine FD d mit $d > 2 \cdot 10^{11}$ und $c^+(d) = 1$.
- b) Es gibt höchstens eine FD d mit $d > 5.2 \cdot 10^{11}$ und $c^+(d) \leq 2$.

Beweis:

- a) Diese Behauptung wird bei (W, Lemma 4, S. 118) bewiesen.
- b) Hier muß etwas genauer als bei (W) argumentiert werden.

Nach (T, Theorem 2, S. 164) gibt es zu $0 < \varepsilon < \frac{1}{2}$ höchstens eine FD d mit $d \geq \max(e^{\frac{4}{\varepsilon}}, e^{11.2})$ und $h^+(d) \leq \frac{0.655}{\pi} \varepsilon d^{\frac{4}{\varepsilon} - \varepsilon}$.

Sei $d \geq d_0 \geq P_r$, $r, d_0 \in \mathbb{N}$, $c^+(d) \leq 2$, $\varepsilon := \frac{1}{\log d_0}$. Falls $d_0 > e^{11.2}$, so folgt für alle d bis auf höchstens ein d

$$(+)\quad h^+(d) > \frac{0.655}{\pi e \log d_0} \sqrt{d_0}$$

Wenn $t = \#\{p \in \mathbb{P} \mid p \mid d\} \geq 11$, so ist

$$d \geq p_{11}^{37^{t-11}} \geq 2 \cdot 10^{11} \cdot 37^{t-11} \quad d_0 \geq p_{11}$$

$$\text{impliziert } \frac{1}{\log p_{11}} \geq \frac{1}{\log d_0} \quad \text{und } p_{11}^{\varepsilon} \leq p_{11}^{\frac{4}{\log p_{11}}} = e,$$

so daß nach (T)

$$(++) \quad h^+(d) > \frac{0.655}{\pi \log d_0} \cdot \frac{\sqrt{p_{11}}}{p_{11}^{\frac{1}{\log p_{11}} d_0}} \cdot 37^{\left(\frac{1}{2}-\varepsilon\right)(t-11)} > \frac{0.655}{\pi e \log d_0} \sqrt{p_{11}} \cdot 37^{\left(\frac{1}{2}-\varepsilon\right)(t-11)}$$

gilt.

Wählt man $d_0 := 5.2 \cdot 10^{11}$, so folgt aus (+) und

$$h^+(d) \leq 2^t, \text{ daß } 2^t > 2^{11}, \text{ also } t \geq 12.$$

Benutzt man andererseits (++), $37^{\frac{1}{2}-\varepsilon} \geq 4$,

$$2^t \geq h^+(d) > 1270.4^{t-11} > 2^{10} 2^{2t-22} = 2^{2t-12},$$

so folgt $t < 12$.

Also führt jedes $d \geq d_0$ - bis auf möglicherweise eine Ausnahme - mit $c^+(d) \leq 2$ zum Widerspruch ●

Mit Hilfe des Computers HB 66/80 im Rechenzentrum Mainz wurde eine Tabelle der Fundamentaldiskriminanten $0 < d \leq 10^7$, $c^+(d) \leq 2$ erstellt (s. S. 66).

Dabei wurden folgende Kriterien benutzt:

- 1) Alle FD $d \leq 100$ mit $c^+(d) \leq 2$ finden sich schnell unter Verwendung der Klassenzahltafel (BS, Tabelle 4, S. 457).
- 2) Satz 49 b), $p = 2$ zeigt $c^+(d) > 2$, falls $d \geq 64$, $d \equiv 7 \pmod{8}$. Zusammen mit den Bedingungen für eine FD d ergibt sich für die Suche der d mit $c^+(d) \leq 2$, daß alle Zahlen $d \equiv 0, 1, 5, 7, 9, 12, 13, 15 \pmod{16}$, $d \equiv 2 \pmod{4}$ gestrichen werden, ebenso alle d mit $p^2 \mid d$, $2 \neq p \in \mathbb{P}$.

3) Die in Satz 49 b) enthaltenen Kongruenzbedingungen werden für $p > 2$ benutzt.

4) Sei $Z = \{ p \in \mathbb{P} \mid 4p^2 \leq d, (\frac{-d}{p}) = 1 \}$, $z = \# Z$.

Dann existiert zu jedem $p \in Z$ ein primitives, nichtambiges Gitter L , $dL = d$ mit $L \ni p$ (vgl. Lemma 48). Die Klasse von L ist durch p eindeutig bestimmt (vgl. Lemma 46, Beweis).

Es gibt also mindestens $2z$ nichtambige engere Klassen in $K^+(d)$.

Andererseits gibt es im Fall $c^+(d) \leq 2$ entweder keine oder 2^{t-1} nichtambige Klassen, so daß

$$2z \leq 2^{t-1}.$$

5) Als letztes Kriterium wurde - falls nötig - Satz 42 verwendet.

Zunächst sucht man ein $p \in \mathbb{P}$, $p \nmid T_b := \frac{d+b^2}{4}$,

$b \equiv 2 \pmod{d}$, $p \nmid d$ mit $4p^2 < d$.

$(p, b, \frac{T_b}{p})$ ist nach Lemma 48 nichtambig.

Nun gilt $n := px^2 + bx + \frac{T_b}{p} \leq \frac{d}{p}$, falls

$$- \left[\frac{b + \sqrt{3d}}{2p} \right] \leq x \leq \left[\frac{-b + \sqrt{3d}}{2p} \right].$$

Wenn $c^+(d) \leq 2$, so sagt Satz 42, daß entweder

$n = p^3$ oder $n|d$ gilt, oder ein $q \in \mathbb{P}$ existiert

mit $q \nmid d$, $q|n$, $\frac{n}{q} \nmid d$.

Im Intervall $[2 \cdot 10^6, 10^7]$ wurden alle FD allein mit den Kriterien 2), 3) und 4) herausgesiebt.

Zwischen 100 und $2 \cdot 10^6$ blieb Kriterium 3) 9525 mal erfolglos, 4) 273 mal und 5) 226 mal erfolglos.

Von diesen 226 Diskriminanten blieben nach Berechnung der Klassengruppe aufgrund von Hilfssatz 41 204 FD übrig. Zusammen mit den 22 FD unterhalb von 100 ergeben sich 226 FD Δ mit $c^+(\Delta) \leq 2$.

Für jede dieser FD können nach Hilfssatz 62 alle f mit $c^+(\Delta \cdot f^2) \leq 2$ bestimmt werden (s. Tabelle S. 66).

67. SATZ: Es gibt 424 Diskriminanten $d = f^2 \Delta$,

$$0 < \Delta \leq 10^7 \text{ mit } c^+(d) \leq 2 .$$

Zu jedem dieser d existieren einklassige Geschlechter.

Insgesamt sind dies 1607 (weitere) Klassen, von denen 439 ambig und 1168 nichtambig sind.

Beweis:

Für jedes d aus der Tabelle wurde die Klassengruppe berechnet.

Im Falle $c^+(d) = 1$ sind alle Klassen ambig und gleich ihrem Geschlecht.

Im Falle $c^+(d) = 2$ haben die nichtambigen Klassen einklassiges Geschlecht. Je zwei solcher engerer Klassen aus $K^+(d)$ bilden eine weitere Klasse ●

Aufgrund des Umfangs können die berechneten Klassen nicht explizit aufgeführt werden. Die folgende Tabelle enthält somit nur die Diskriminanten.

Tabelle der Diskriminanten $d > 0$, $d = \Delta(d) f^2$, $f \in \mathbb{N}$,
 $0 < \Delta(d) \leq 10^7$, für die ein binäres positiv-definites
 primitives $\mathbb{Z}$ -Gitter L mit einklassigem Geschlecht existiert:

Δ	$c^+(d) = 1$ f	$c^+(d) = 2$ f	Δ	$c^+(d) = 1$ f	$c^+(d) = 2$ f
3	1,2,3,4,5, 7,8	11,13	88	1,2	3,4,6
4	1,2,3,4,5	6,7,8,10,12, 15,20	91	1	3,5
7	1,2,4,8	3,6,12,16,24	115	1	3
8	1,2,3,6	4,12	120	1,2	4
11	1,3	5,15	123	1	-
15	1,2,4,8	16	132	1	2,4
19	1	3,5	136	-	1,2
20	1,3	2,4,6,12	148	1	2,3,4
24	1,2	4,5,10	155	-	1,3
35	1,3	-	163	1	3
39	-	1,2,4,8	168	1,2	4
40	1,2	3,4,6	184	-	1,2
43	1	3	187	1	3
51	1	5	195	1	-
52	1	2,3,4	203	-	1,3
55	-	1,2,4,8	219	-	1
56	-	1,2,3,6	228	1	2,4
67	1	3	232	1,2	3,4,6
68	-	1,3	235	1	3
84	1	2,4,5	259	-	1

Δ	$c^+(d) = 1$ f	$c^+(d) = 2$ f	Δ	$c^+(d) = 1$ f	$c^+(d) = 2$ f
260	-	1,3	555	1	-
264	-	1,2	564	-	1
267	1	-	568	-	1,2
276	-	1	580	-	1
280	1,2	3,4,6	595	1	3
291	-	1	616	-	1,2
292	-	1	627	1	-
308	-	1,3	651	-	1
312	1,2	4	660	1	2,4
323	-	1,3	667	-	1
328	-	1,2	708	1	2,4
340	1	2,3,4	715	1	3
355	-	1	723	-	1
372	1	2,4	760	1,2	3,4,6
388	-	1	763	-	1
403	1	3	772	-	1
408	1,2	4	795	1	-
420	1	2,4	820	-	1
427	1	3	840	1,2	4
435	1	-	852	-	1
456	-	1,2	868	-	1
483	1	-	915	-	1
520	1,2	3,4,6	952	-	1,2
532	1	2,3,4	955	-	1
552	-	1,2	987	-	1

Δ	$c^+(d) = 1$ f	$c^+(d) = 2$ f	Δ	$c^+(d) = 1$ f	$c^+(d) = 2$ f
1003	-	1	1560	-	1,2
1012	1	2,3,4	1635	-	1
1027	-	1	1659	-	1
1032	-	1,2	1672	-	1,2
1060	-	1	1716	-	1
1092	1	2,4	1752	-	1,2
1128	-	1,2	1768	-	1,2
1131	-	1	1771	-	1
1140	-	1	1780	-	1
1155	1	-	1848	1,2	4
1204	-	1	1860	-	1
1227	-	1	1947	-	1
1240	-	1,2	1992	-	1,2
1243	-	1	1995	1	-
1288	-	1,2	2020	-	1
1320	1,2	4	2035	-	1
1380	1	2,4	2040	-	1,2
1387	-	1	2067	-	1
1411	-	1	2139	-	1
1428	1	2,4	2163	-	1
1435	1	3	2212	-	1
1443	-	1	2244	-	1
1507	-	1	2280	-	1,2
1540	1	2,3,4	2392	-	1,2
1555	-	1	2436	-	1

Δ	$c^+(d) = 1$ f	$c^+(d) = 2$ f	Δ	$c^+(d) = 1$ f	$c^+(d) = 2$ f
2451	-	1	4123	-	1
2580	-	1	4180	-	1
2632	-	1,2	4260	-	1
2667	-	1	4323	-	1
2715	-	1	4420	-	1
2755	-	1	4440	-	1,2
2760	-	1,2	4452	-	1
2788	-	1	4488	-	1,2
2968	-	1,2	4515	-	1
3003	1	-	4740	-	1
3108	-	1	5083	-	1
3172	-	1	5115	-	1
3192	-	1,2	5160	-	1,2
3220	-	1	5187	-	1
3243	-	1	5208	-	1,2
3315	1	-	5412	-	1
3355	-	1	5460	1	2,4
3432	-	1,2	5467	-	1
3480	-	1,2	6195	-	1
3507	-	1	6307	-	1
3588	-	1	6420	-	1
3640	-	1,2	6580	-	1
3795	-	1	6612	-	1
3828	-	1	6708	-	1
4020	-	1	6820	-	1

Δ	$c^+(d) = 1$ f	$c^+(d) = 2$ f	Δ	$c^+(d) = 1$ f	$c^+(d) = 2$ f
7035	-	1	10920	-	1,2
7140	-	1	10948	-	1
7315	-	1	11067	-	1
7395	-	1	11715	-	1
7480	-	1,2	12180	-	1
7540	-	1	13195	-	1
7755	-	1	14280	-	1,2
7995	-	1	14763	-	1
8008	-	1,2	14820	-	1
8052	-	1	16555	-	1
8547	-	1	17220	-	1
8580	-	1	19320	-	1,2
8680	-	1,2	19380	-	1
8715	-	1	19635	-	1
8835	-	1	20020	-	1
8932	-	1	31395	-	1
9240	-	1,2	33915	-	1
9867	-	1	40755	-	1

Literaturverzeichnis

- B-Sch Baker, A., Schinzel, A., On the least integers represented by the genera of binary quadratic forms, Acta Arith. 18 (1971), S. 137 - 144.
- BS Borewics, S.I., Safarewic, I.R., Zahlentheorie, Basel u. Stuttgart 1966.
- Ch Chowla, S., An extension of Heilbronn's class-numbertheorem, Quat. J. Math. 5 (1934), S. 304 - 307.
- CB Chowla, S., Briggs, W.E., On discriminants of binary quadratic forms with a single class in each genus, Canad. J. Math. 6 (1954), S. 463 - 470.
- G Gauss, C.F., Disquisitiones arithmeticae, 1801, Art. 303.
- Gro Grosswald, E., Negative discriminants of binary quadratic forms with one class in each genus, Acta Arith. 8 (1963), S. 295 - 306.
- Gr Grube, F., Über einige Eulersche Sätze aus der Theorie der quadratischen Formen, Zeitschr. für Math. u. Phys., 19 (1874), S. 492 - 519.
- H Hall, N.A., Binary quadratic discriminants with a single class of forms in each genus, Math. Zeitschr., 44 (1939), S. 85 - 90.
- J Jones, B.W., The arithmetic theory of quadratic forms, Baltimore 1950.

- K Kneser, M., Quadratische Formen, Vorlesungsausarbeitung, Math. Inst. d. Universität Göttingen, SS 1973, WS 1973/74.
- L Landau, E., Vorlesungen über Zahlentheorie, Bd. 1, Leipzig 1927.
- M Möller, H., Imaginär-quadratische Zahlkörper mit einklassigen Geschlechtern, Acta Arith. 30 (1976), S. 179 - 186.
- N Narkiewicz, W., Elementary and analytic theory of algebraic numbers, Warszawa 1974.
- OM O'Meara, D.T., Introduction to quadratic forms, 3. Aufl., Berlin, Heidelberg, New York 1973.
- P Pfeuffer, H., Einklassige Geschlechter total-positiver quadratischer Formen in totalreellen algebraischen Zahlkörpern, J. of Number Theory, Vol. 3 (1971), S. 371 - 411.
- Sch Schinzel, A., Sur les sommes de trois carrés, Bull. de l'Acad. Pol. de Sc., Ser. sci. math., astr. et phys., Vol. VII, No. 6 (1959), S. 308 - 310.
- S Siegel, C.L., Über die Classenzahl quadratischer Zahlkörper, Acta Arith. 1 (1935), S. 83 - 86.
- St Steinig, J., On Eulers idoneal numbers, Elemente d. Math. 21 (1966), S. 73 - 96.
- Sw Swift, J.D., Note on discriminants of binary quadratic forms with a single class in each genus, Bull. Am. Math. Soc. 54 (1948), S. 560/561.

- T Tatzuza, T., On a theorem of Siegel, Japan J. Math. 21 (1951), S. 163 - 177.
- vdW Waerden, B.L.v.d., Die Reduktionstheorie der positiven quadratischen Formen, Acta Math. 96 (1956), S. 266 - 309.
- W1 Watson, G.L., Transformations of a quadratic form which do not increase the classnumber, Proc. London Math. Soc. (3) 12 (1962), S. 577 - 587.
- W2 derselbe, Transformations of a quadratic form which do not increase the classnumber (II), Acta Arith. 27 (1975), S. 171 - 189.
- W3 derselbe, The classnumber of a positiv quadratic form, Proc. London Math. Soc. (3) 13 (1963), S. 549 - 576.
- W4 derselbe, Regular, positive, ternary quadratic forms, J. London Math. Soc. (2) 13 (1976), S. 97 - 102.
- W5 derselbe, Positive quadratic forms with small classnumbers, Proc. London Math. Soc. (3) 13 (1963), S. 577 - 592.
- W6 derselbe, One-class genera of positive quadratic forms, J. London Math. Soc. 38 (1963), S. 387 - 392.
- W7 derselbe, One-class genera of positive ternary quadratic forms, Mathematika 19 (1972), S. 96 - 104.
- W8 derselbe, One-class genera of positive quaternary quadratic forms, Acta Arith. 24 (1973), S. 461 - 475.

- W9 derselbe, One-class genera of positive quadratic forms in at least five variables, Acta Arith. 26 (1975), S. 309 - 327.
- W10 derselbe, One-class genera of positive ternary quadratic forms II, Mathematika 22 (1975), S. 1 - 11.
- We Weinberger, P.J., Exponents of the class groups of complex quadratic fields, Acta Arith. 22 (1973), S. 117 - 124.
- Web Weber, H., Beweis des Satzes, daß jede eigentlich primitive quadratische Form unendlich viele Primzahlen darstellt, Math. Ann. 20 (1882), S. 301 - 329.

Lebenslauf

Am 7. November 1953 wurde ich in Simmern (Hunsrück) als Sohn des Kaufmanns Artur Kassner und dessen Ehefrau Karoline geb. Simson geboren. Die Grundschule besuchte ich seit 1960 in Kastellaun. 1964 folgte der Eintritt in das Herzog-Johann-Gymnasium in Simmern, wo ich im Mai 1972 mit dem Abitur abschloß. Im Oktober desselben Jahres begann ich mit dem Studium der Mathematik und Physik an der Johannes Gutenberg-Universität in Mainz; die Vordiplomprüfung erfolgte im Oktober 1974, die Diplomprüfung im Fach Mathematik drei Jahre später. Bis Oktober 1978 übte ich am Fachbereich Mathematik in Mainz eine Tätigkeit als wissenschaftliche Hilfskraft aus und trat dann die Stelle eines wissenschaftlichen Mitarbeiters an. Meine Frau Gabriele geb. Meurer heiratete ich im Juli 1979. Im November 1980 kam unser Sohn Sebastian zur Welt. Am 23. Juni 1981 legte ich am Fachbereich Mathematik in Mainz die Promotionsprüfung ab.

Michael Kassner
Schulstr. 5
6544 Kirchberg

